Manuale sul diritto europeo in materia di protezione dei dati

1.1. Il diritto alla protezione dei dati di carattere personale

- Ai sensi dell’articolo 8 della CEDU, il diritto alla protezione per quanto riguarda il trattamento dei dati personali è parte del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.

- La Convenzione n. 108 del CdE è il primo, e ad oggi l’unico, strumento internazionale giuridicamente vincolante che tratta della protezione dei dati. La Convenzione è stata oggetto di un processo di modernizzazione, completato con l'adozione del Protocollo di modifica il 18 aprile 2018.

- Il diritto dell’UE ha riconosciuto la protezione dei dati come un diritto fondamentale distinto. Ciò è sancito dall’articolo 16 del trattato sul funzionamento dell’Unione europea nonché dall’articolo 8 della Carta dei diritti fondamentali dell’UE.

- Il diritto dell’UE ha disciplinato per la prima volta la protezione dei dati attraverso la direttiva sulla tutela dei dati nel 1995.

- Alla luce dei rapidi sviluppi tecnologici, nel 2016 l’UE ha adottato una nuova legi- slazione per

adeguare le norme in materia di protezione dei dati all'era digitale. Il regolamento generale sulla protezione dei dati è diventato applicabile nel maggio 2018, abrogando la direttiva sulla tutela dei dati.

- Contestualmente al regolamento generale sulla protezione dei dati, l'UE ha adot- tato una legislazione sul trattamento dei dati personali da parte delle autorità statali a fini di contrasto alla criminalità. La direttiva (UE) 2017/680 stabilisce norme e principi in materia di protezione dei dati che disciplinano il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

1.1.1. Il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali: una breve introduzione

Il diritto al rispetto della vita privata e il diritto alla protezione dei dati per- sonali, sebbene strettamente connessi, sono diritti distinti. Nel diritto inter- nazionale in materia di diritti umani, il diritto alla vita privata, conosciuto nel diritto europeo come diritto al rispetto della vita privata, è stato sancito dalla dichiarazione universale dei diritti dell'uomo (UDHR), adottata nel 1948, come uno dei diritti umani fondamentali protetti. Poco dopo l'adozione di tale dichia- razione, anche l'Europa ha sancito questo diritto, nella Convenzione europea dei diritti dell'uomo (CEDU), un trattato giuridicamente vincolante per le parti contraenti, redatto nel 1950. La CEDU stabilisce che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della pro-

pria corrispondenza. L’ingerenza di un’autorità pubblica in questo diritto è vie- tata, eccetto nei casi in cui sia prevista dalla legge, persegua interessi pubblici importanti e legittimi e sia necessaria in una società democratica.

L’UDHR e la CEDU sono state adottate ben prima dello sviluppo dei compu- ter e di Internet e dell’avvento della società dell’informazione. Questi sviluppi hanno apportato significativi vantaggi alle persone e alla società, migliorando la qualità della vita, l’efficienza e la produttività. Al contempo, essi presentano nuovi rischi per il diritto al rispetto della vita privata. In risposta alla neces- sità di norme specifiche a disciplina della raccolta e dell’utilizzo di informazioni personali, è emerso un nuovo concetto di vita privata, noto in alcune giuri- sdizioni come diritto all’«autodeterminazione informativa»[1]. Questo concetto

ha portato allo sviluppo di normative specifiche, che offrono la protezione dei dati personali.

La protezione dei dati in Europa è iniziata negli anni ’70 con l’adozione di una normativa, da parte di alcuni Stati, finalizzata a controllare il trattamento dei dati personali da parte delle autorità pubbliche e delle grandi imprese[2]. Sono quindi stati creati strumenti per la tutela dei dati a livello europeo[3] e, nel corso degli anni, la protezione dei dati si è evoluta fino a diventare un valore distinto, che non può essere classificato come diritto al rispetto della vita privata. Nell’ordinamento giuridico dell’UE, la protezione dei dati è riconosciuta come un diritto fondamentale, distinto dal diritto fondamentale al rispetto della vita privata. Questa distinzione solleva la questione del rapporto e delle differenze tra i due diritti.

Il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali sono strettamente connessi. Entrambi mirano a proteggere valori simili, vale a dire l’autonomia e la dignità umana delle persone, accordando loro una sfera personale nella quale possano sviluppare liberamente la loro personalità, pen- sare e modellare le loro opinioni. Essi costituiscono, pertanto, un presupposto essenziale per l’esercizio di altre libertà fondamentali, quali la libertà di espres- sione, la libertà di riunione pacifica e di associazione, e la libertà di religione.

I due diritti differiscono in termini di formulazione e portata. Il diritto al rispetto della vita privata consiste in un divieto generale di ingerenza, assoggettato ad alcuni criteri di interesse pubblico che possono giustificare l'ingerenza in deter- minati casi. La protezione dei dati personali è vista come un diritto moderno e attivo[4], che instaura un sistema di controlli ed equilibri volti a proteggere le persone ogni qualvolta siano trattati i loro dati personali. Il trattamento deve

essere conforme agli elementi essenziali della protezione dei dati personali, segnatamente il controllo indipendente e il rispetto dei diritti dell'interessato[5].

L'articolo 8 della Carta dei diritti fondamentali dell'UE (la «Carta») non si limita a sancire il diritto alla protezione dei dati personali, ma enuncia anche i valori fondamentali associati a tale diritto. Esso stabilisce che il trattamento dei dati personali deve avvenire secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o su un fondamento legittimo previsto dalla legge. Le persone devono avere il diritto di accedere ai propri dati personali e di ottenerne la rettifica, e il rispetto di tale diritto deve essere soggetto al controllo di un'autorità indipendente.

Il diritto alla protezione dei dati personali entra in gioco ogni volta che ven- gono trattati dati personali; è quindi più ampio del diritto al rispetto della vita privata. Tutte le operazioni di trattamento dei dati personali sono soggette a una protezione adeguata. La protezione dei dati riguarda tutti i tipi di dati per- sonali e trattamento dei dati, indipendentemente dal rapporto e dall'impatto sulla vita privata. Il trattamento dei dati personali può altresì pregiudicare il diritto alla vita privata, come illustrato negli esempi che seguono. Tuttavia, non è necessario dimostrare una violazione della vita

privata perché siano applica- bili le norme sulla protezione dei dati.

Il diritto alla vita privata riguarda situazioni in cui siano stati compromessi un interesse privato o la «vita privata» di una persona. Come dimostrato nel presente manuale, la nozione di «vita privata» è stata interpretata in senso ampio nella giurisprudenza, nel senso che essa comprende situazioni di natura intima, informazioni sensibili o riservate, informazioni che potrebbero pregiu- dicare la percezione del pubblico nei confronti di un individuo, e perfino aspetti della vita professionale e del comportamento pubblico di una persona. Tutta- via la valutazione circa l'esistenza o meno di un'ingerenza nella «vita privata» dipende dal contesto e dalle circostanze di ciascun caso.

Per contro, qualsiasi operazione che comporti il trattamento di dati personali potrebbe rientrare nell'ambito di applicazione delle norme in materia di prote- zione dei dati e far sorgere il diritto alla protezione dei dati personali. Ad esem- pio, se un datore di lavoro registra informazioni relative ai nomi e alle retribu- zioni corrisposte ai dipendenti, la mera registrazione di tali informazioni non può

essere considerata un’ingerenza nella vita privata. Tale ingerenza potrebbe tut- tavia essere invocata, ad esempio, qualora il datore di lavoro trasferisse a terzi informazioni personali riguardanti i dipendenti. I datori di lavoro devono in ogni caso rispettare le norme sulla protezione dei dati, in quanto la registrazione di informazioni riguardanti i dipendenti costituisce trattamento dei dati.

Esempio: nella causa *Digital Rights Ireland*[6], la CGUE è stata chiamata a pronunciarsi sulla validità della direttiva 2006/24/CE sotto il profilo dei diritti fondamentali alla protezione dei dati personali e al rispetto della vita privata, sanciti dalla Carta dei diritti fondamentali dell’UE. La direttiva imponeva ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione di conservare i dati delle telecomunicazioni dei cittadini per un periodo di due anni, a fini di prevenzione, indagine e perseguimento di reati gravi. La misura riguardava solo i metadati, i dati relativi all’ubicazione e i dati necessari per identificare l’abbonato o l’utente. Non era applicabile al contenuto delle comunicazioni elettroniche.

La CGUE ha considerato la direttiva un’ingerenza nel diritto fondamentale alla protezione dei dati personali «poiché prevede un trattamento dei dati personali»[7]. Ha inoltre constatato che la direttiva

interferiva nel diritto al rispetto della vita privata[8]. Presi nel loro complesso, i dati personali conservati a norma della direttiva, che erano accessibili alle autorità competenti, potevano permettere di trarre «conclusioni molto precise riguardo alla vita privata delle persone i cui dati [erano] stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati»[9]. L'ingerenza nei due diritti era di vasta portata e particolarmente grave.

La Corte di giustizia ha dichiarato invalida la direttiva 2006/24/CE, concludendo che, malgrado la stessa perseguisse un obiettivo legittimo, l'ingerenza nei diritti alla protezione dei dati personali e alla vita privata era grave e non limitata a quanto strettamente necessario.

1.1.2. Quadro giuridico internazionale: le Nazioni Unite

Il quadro delle Nazioni Unite non riconosce la protezione dei dati personali come diritto fondamentale, anche se il diritto alla vita privata è un diritto fon- damentale consolidato nell'ordinamento giuridico internazionale. Il diritto delle persone alla protezione della sfera privata contro le ingerenze altrui, soprat- tutto da parte dello Stato, è stato sancito per la prima volta da uno strumento internazionale nell'articolo 12 dell'UDHR, riguardante il rispetto della vita pri- vata e familiare[10]. L'UDHR, pur essendo una dichiarazione non vincolante, gode di uno status considerevole quale strumento fondamentale del diritto interna- zionale dei diritti umani, e ha influenzato lo sviluppo di altri strumenti relativi ai diritti umani in Europa. Il Patto internazionale relativo ai diritti civili e politici (ICCPR), entrato in vigore nel 1976, stabilisce che nessuno può essere sottopo- sto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua casa o nella sua corrispondenza né a illegittime offese al suo onore e alla sua repu- tazione. L'ICCPR è un trattato internazionale che impegna le 169 parti contra- enti a rispettare e garantire l'esercizio dei diritti civili delle persone, compresa la vita privata.

Dal 2013, le Nazioni Unite adottano due risoluzioni su questioni concernenti la vita privata intitolate «The right to privacy in the digital age»[11] [il diritto alla vita privata nell'era digitale], in risposta allo

sviluppo di nuove tecnologie e alle rivelazioni sulla sorveglianza di massa effettuata in alcuni Stati (le rivelazioni di Snowden). Tali risoluzioni condannano fermamente la sorveglianza di massa ed evidenziano l'impatto che tale sorveglianza può avere sui diritti fondamentali alla vita privata e alla libertà di espressione nonché sul funzionamento di una società democratica e dinamica. Sebbene non giuridicamente vincolanti, esse hanno suscitato un importante dibattito politico internazionale di alto livello in materia di vita privata, nuove tecnologie e sorveglianza. Hanno altresì portato all'istituzione di un relatore speciale sul diritto alla vita privata, con il mandato di promuovere e tutelare tale diritto. Le funzioni specifiche del relatore com- prendono la raccolta di informazioni sulle prassi e sulle esperienze nazionali in materia di vita privata e le sfide derivanti dalle nuove tecnologie, lo scambio la promozione delle migliori pratiche e l'individuazione di potenziali ostacoli.

Mentre le risoluzioni precedenti convergevano sugli effetti negativi della sor- veglianza di massa e sulla responsabilità degli Stati di limitare i poteri delle autorità di intelligence, le risoluzioni più recenti riflettono uno sviluppo fon- damentale nel dibattito sulla vita privata nelle Nazioni Unite[12]. Le risoluzioni adottate nel 2016 e nel 2017 riaffermano la necessità di limitare i poteri delle agenzie di intelligence e di condannare la sorveglianza di massa. Tuttavia, esse affermano altresì esplicitamente che «le crescenti capacità delle imprese di raccogliere, trattare e utilizzare dati personali possono rappresentare un rischio per il godimento del diritto alla vita privata nell'era digitale». Pertanto, oltre alla responsabilità delle autorità statali, le risoluzioni sottolineano la respon- sabilità del settore privato nel rispetto dei diritti umani e invitano le imprese a informare gli utilizzatori in merito alla raccolta, all'utilizzo, alla condivisione e alla conservazione dei dati personali nonché a prevedere politiche di tratta- mento trasparenti.

1.1.3. La Convenzione europea dei diritti dell'uomo

Il Consiglio d'Europa è stato costituito all'indomani della seconda guerra mon- diale con l'obiettivo di riunire gli Stati d'Europa e promuovere lo Stato di diritto, la democrazia, i diritti dell'uomo e lo sviluppo

sociale. A tal fine, nel 1950 esso ha adottato la CEDU, entrata in vigore nel 1953.

Le parti contraenti hanno l'obbligo internazionale di attenersi alla CEDU. Tutti gli Stati membri del CdE hanno ormai recepito o dato efficacia alla CEDU nel rispettivo diritto nazionale, che impone loro di agire conformemente alle dispo- sizioni contenute nella stessa. Le parti contraenti devono rispettare i diritti stabiliti nella Convenzione nell'esercizio di qualsiasi attività o potere. Questo comprende le attività intraprese a fini di sicurezza nazionale. Sentenze cardine della Corte europea dei diritti dell'uomo (Corte EDU) riguardano attività sta- tali in settori sensibili della legislazione e della prassi in materia di sicurezza nazionale[13]. La Corte non ha esitato ad affermare che le attività di sorveglianza interferiscono nel rispetto per la vita privata[14].

Per garantire che le parti contraenti adempiano i propri obblighi ai sensi della CEDU, nel 1959 è stata istituita a Strasburgo (Francia) la Corte EDU. La Corte EDU garantisce che gli Stati adempiano gli obblighi previsti dalla Convenzione valutando le denunce presentate da singoli individui, gruppi di individui, ONG o persone giuridiche che asseriscano l'esistenza di violazioni della Convenzione. La Corte EDU può altresì esaminare le cause interstatali intentate da uno o più Stati membri del CdE contro un altro Stato membro.

Al 2018 il Consiglio d'Europa è formato da 47 parti contraenti, 28 delle quali sono anche Stati membri dell'UE. Per adire la Corte EDU non è necessario essere cittadino di una delle parti contraenti, anche se le presunte violazioni devono aver luogo all'interno della giurisdizione di una delle parti contraenti.

Il diritto alla protezione dei dati personali rientra nei diritti tutelati dall'arti- colo 8 della CEDU, che garantisce il diritto al rispetto della vita privata e fami- liare, del domicilio e della corrispondenza, e stabilisce le condizioni alle quali tale diritto può essere soggetto a restrizioni[15].

La Corte EDU ha esaminato numerose situazioni in materia di protezione dei dati, non ultime quelle riguardanti l'intercettazione di comunicazioni[16], varie forme di sorveglianza da parte sia del settore

privato sia del settore pubblico[17], nonché le garanzie rispetto alla conservazione dei dati personali da parte delle autorità pubbliche[18]. Atteso che il rispetto della vita privata non è un diritto assoluto, qualora l'esercizio del diritto alla vita privata possa compromettere altri diritti, come la libertà di espressione e l'accesso alle informazioni, e vice- versa, la Corte si adopera per trovare un equilibrio tra i diversi diritti in gioco. Essa ha chiarito che l'articolo 8 della CEDU non solo obbliga gli Stati ad aste- nersi da qualsiasi azione che potrebbe violare questo diritto previsto dalla Con- venzione, ma impone loro altresì, in talune circostanze, l'obbligo di garantire attivamente l'effettivo rispetto della vita privata e familiare[19]. I capitoli perti- nenti descrivono molti di questi casi in modo dettagliato.

1.1.4. La Convenzione n. 108 del Consiglio d'Europa

L'emergere delle tecnologie dell'informazione negli anni '60 ha determinato un crescente bisogno di norme più dettagliate per tutelare le persone proteggen- done i dati personali. A metà degli anni '70, il Comitato dei Ministri del Consi- glio d'Europa ha adottato varie risoluzioni in materia di protezione dei dati per- sonali, facendo riferimento all'articolo 8 della CEDU[20]. Nel 1981 è stata aperta alla firma una Convenzione sulla protezione delle persone rispetto al tratta- mento automatizzato di dati a carattere personale (Convenzione n. 108)[21]. La Convenzione n. 108 era, e rimane, l'unico strumento internazionale giuridica- mente vincolante in materia di protezione dei dati.

La Convenzione n. 108 si applica a tutti i trattamenti di dati personali effet- tuati sia nel settore privato che nel pubblico, compresi quelli effettuati da auto- rità giudiziarie e di polizia. Essa protegge gli individui dagli abusi che possono accompagnare il trattamento dei dati personali e, nel contempo, cerca di rego- lamentare i flussi transfrontalieri di dati personali. Per quanto concerne il trat- tamento dei dati personali, i principi stabiliti nella Convenzione riguardano, in particolare, la correttezza e la liceità della raccolta e del trattamento automa- tizzato dei dati, per specifici scopi legittimi. Ciò significa che i dati non devono essere destinati a un uso incompatibile con tali

scopi, né conservati oltre il tempo necessario. Tali principi riguardano anche la qualità dei dati, in partico- lare in riferimento alla loro adeguatezza, pertinenza e non eccessività (propor- zionalità) nonché esattezza.

Oltre a fornire garanzie sul trattamento dei dati personali e gli obblighi relativi alla sicurezza dei dati, la Convenzione, in assenza di adeguate garanzie giuri- diche, vieta il trattamento dei dati «sensibili», come la razza, le opinioni poli- tiche, la salute, la religione, l'orientamento sessuale o il casellario giudiziale di un individuo.

La Convenzione sancisce inoltre il diritto dell'individuo di essere informato della conservazione di informazioni che lo riguardano e di chiederne la rettifica, se del caso. Le restrizioni dei diritti stabiliti nella Convenzione sono possibili solo quando sono in gioco interessi superiori, quali la sicurezza o la difesa dello

Stato. Inoltre, la Convenzione prevede la libera circolazione dei dati personali tra le parti contraenti e impone alcune restrizioni su tali flussi verso paesi in cui la regolamentazione giuridica non conferisce una protezione equivalente.

Va osservato che la Convenzione n. 108 è vincolante per gli Stati che l'hanno ratificata. Essa non è soggetta al controllo giudiziario della Corte EDU, ma è stata tenuta in considerazione nella giurisprudenza della Corte EDU, nel quadro dell'articolo 8 della CEDU. Nel corso degli anni, la Corte ha stabilito che la prote- zione dei dati personali è una parte importante del diritto al rispetto della vita privata (articolo 8), e si è ispirata ai principi della Convenzione n. 108 per deter- minare se vi sia stata o meno un'ingerenza in questo diritto fondamentale[22].

Per sviluppare ulteriormente i principi generali e le norme previste dalla Con- venzione n. 108, il Comitato dei Ministri del CdE ha adottato diverse racco- mandazioni giuridicamente non vincolanti. Queste raccomandazioni hanno influenzato lo sviluppo del diritto in materia di protezione dei dati in Europa. Ad esempio, per anni, l'unico strumento di orientamento in Europa riguardante l'u- tilizzo dei dati personali in ambito di polizia è stata la raccomandazione relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza[23]. I principi contenuti nella raccomandazione, come i mezzi per conservare i file di dati e la necessità di

stabilire norme chiare sulle persone autorizzate ad accedere a tali file, sono stati ulteriormente sviluppati e sono stati ripresi nella successiva legislazione dell'UE[24]. Raccomandazioni più recenti sono volte ad affrontare le sfide dell'era digitale, ad esempio, in relazione al trattamento dei dati nel contesto dell'occupazione (cfr. capitolo 9).

Tutti gli Stati membri dell'UE hanno ratificato la Convenzione n. 108, che nel 1999 è stata emendata per consentire all'UE di diventarne parte contra- ente[25]. Nel 2001 è stato adottato un Protocollo addizionale alla Convenzione n.

108, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti, i cosiddetti paesi terzi, e l'istituzione obbligatoria delle autorità nazionali di controllo per la protezione dei dati[26].

La Convenzione n. 108 è aperta all'adesione delle parti non contraenti del CdE. La portata della Convenzione come norma universale e il suo carattere aperto potrebbero costituire un presupposto per promuovere la protezione dei dati a livello mondiale. Ad oggi, 50 paesi sono parti contraenti della Convenzione n. 108. Essi comprendono tutti gli Stati membri del Consiglio d'Europa (47 paesi), l'Uruguay, il primo paese extraeuropeo che vi ha aderito, nell'agosto 2013, e Maurizio, Senegal e la Tunisia che vi hanno aderito nel 2016 e nel 2017.

La Convenzione è stata recentemente oggetto di un processo di moderniz- zazione. Una consultazione pubblica effettuata nel 2011 ha confermato i due obiettivi principali di tale lavoro: il rafforzamento della protezione della vita privata nel settore digitale e il consolidamento del meccanismo di attuazione della Convenzione. Il processo di modernizzazione era incentrato su tali obiet- tivi ed è stato completato il 18 aprile 2018 con l'adozione del protocollo di modifica della Convenzione n. 108 (Protocollo CETS No. 223). Il lavoro è stato svolto parallelamente ad altre riforme degli strumenti

internazionali di prote- zione dei dati e contestualmente alla riforma della legislazione dell'UE sulla protezione dei dati, avviata nel 2012. I legislatori presso il Consiglio d'Europa e a livello dell'UE hanno posto massima attenzione nell'assicurare la coerenza e la compatibilità tra i due quadri normativi. La modernizzazione mantiene il carattere generale e flessibile della Convenzione e ne rafforza il potenziale come strumento universale sul diritto in materia di protezione dei dati. Essa riafferma e consolida importanti principi e prevede nuovi diritti a vantaggio degli individui, ampliando al contempo le responsabilità delle entità preposte al trattamento dei dati personali e assicurando maggiore responsabilità. Ad esempio, le persone i cui dati vengono trattati hanno il diritto di venire a cono- scenza del motivo di tale trattamento dei dati e il diritto di opporsi allo stesso. Per contrastare l'aumento dell'attività di profilazione nel mondo online, la Con- venzione sancisce altresì il diritto dell'individuo a non essere assoggettato a decisioni fondate esclusivamente su trattamenti automatizzati, senza che siano prese in considerazione le sue opinioni. L'efficace applicazione delle norme in materia di protezione dei dati da parte di autorità di controllo indipendenti

nelle parti contraenti è considerata essenziale per l'attuazione pratica della Convenzione. A tal fine, la Convenzione modernizzata sottolinea la necessità che le autorità di controllo siano dotate di poteri e funzioni efficaci e godano di un'autentica indipendenza nell'adempimento della loro missione.

1.1.5. Il diritto dell'Unione europea in materia di protezione dei dati

Il diritto dell'Unione europea si compone del diritto primario e derivato dell'UE. I trattati, vale a dire il trattato sull'Unione europea (TUE) e il trattato sul funzio- namento dell'Unione europea (TFUE) sono stati ratificati da tutti gli Stati mem- bri dell'UE e formano il «diritto primario dell'UE». I regolamenti, le direttive e le decisioni dell'UE, adottati dalle istituzioni dell'UE alle quali è stata conferita tale autorità in virtù dei trattati, costituiscono il «diritto derivato dell'UE».

La protezione dei dati nel diritto primario dell'UE

I trattati originari delle Comunità europee non contenevano riferimenti ai diritti umani o alla loro protezione, in quanto inizialmente la Comunità economica europea era considerata un'organizzazione regionale volta all'integrazione eco- nomica e all'istituzione di un mercato comune. Un principio fondamentale alla base della creazione e dello sviluppo delle Comunità europee, altrettanto

valido oggi, è il principio dell'attribuzione. In virtù di tale principio, l'UE agisce esclusi- vamente nei limiti delle competenze che le sono attribuite dagli Stati membri, come sancito dai trattati dell'UE. Contrariamente al Consiglio d'Europa, i trattati dell'UE non prevedono competenze esplicite in materia di diritti fondamentali.

Quando, tuttavia, la CGUE è stata chiamata a pronunciarsi su cause relative a vio- lazioni dei diritti umani in contesti rientranti nell'ambito di applicazione del diritto dell'UE, essa ha fornito un'importante interpretazione dei trattati. Per garantire protezione alle persone, la CGUE ha introdotto i diritti fondamentali nei cosid- detti principi generali del diritto europeo. Secondo la CGUE, tali principi generali riflettono la protezione dei diritti umani garantita dalle costituzioni nazionali e dai trattati sui diritti umani, in particolare la CEDU. La CGUE ha espresso il proprio impegno a garantire la conformità del diritto dell'UE a tali principi.

Consapevole delle eventuali ripercussioni delle sue politiche sui diritti umani e nel tentativo di far sentire i cittadini «più vicini» all'Unione, nel 2000 l'UE ha

proclamato la Carta dei diritti fondamentali dell'Unione europea (la «Carta»). Essa incorpora la totalità dei diritti civili, politici, economici e sociali dei cittadini europei, sintetizzando le tradizioni costituzionali e gli obblighi internazionali comuni agli Stati membri. I diritti descritti nella Carta sono suddivisi in sei titoli: dignità, libertà, uguaglianza, solidarietà, cittadinanza e giustizia.

Trattandosi inizialmente solo di un documento politico, la Carta è divenuta giuridi- camente vincolante[27] come diritto primario dell'UE (cfr. l'articolo 6, paragrafo 1, del TUE) con l'entrata in vigore del trattato di Lisbona il 1° dicembre 2009[28]. Le dispo- sizioni della Carta si applicano alle istituzioni e agli organi dell'UE e impongono loro il rispetto dei diritti ivi elencati nell'adempimento dei loro doveri. Le disposizioni della Carta vincolano anche gli Stati membri nell'attuazione del diritto dell'UE.

La Carta non solo garantisce il rispetto della vita privata e della vita familiare (articolo 7), ma stabilisce anche il diritto alla protezione dei dati di carattere personale (articolo 8), innalzando esplicitamente il livello di tale protezione a quello di un diritto fondamentale nell'ambito del diritto dell'UE. Le istituzioni e gli organi dell'UE devono garantire e rispettare tale diritto, come pure gli Stati membri nell'attuazione del diritto dell'Unione (articolo 51 della Carta). Formu- lato diversi anni dopo la direttiva sulla tutela dei dati, l'articolo 8

della Carta deve essere inteso come recante il diritto dell'UE preesistente in materia di protezione dei dati. La Carta, dunque, non solo menziona esplicitamente, all'ar- ticolo 8, paragrafo 1, il diritto alla protezione dei dati, ma all'articolo 8, para- grafo 2, fa altresì riferimento ai principi fondamentali della protezione dei dati. Infine, l'articolo 8, paragrafo 3, della Carta esige che un'autorità indipendente controlli l'attuazione di questi principi.

L'adozione del trattato di Lisbona è una pietra miliare nello sviluppo della legi- slazione in materia di protezione dei dati, non solo per avere elevato la Carta allo status di documento legale vincolante a livello di diritto primario, ma anche per avere previsto il diritto alla protezione dei dati personali. Questo diritto è specificamente contemplato all'articolo 16 del TFUE, nella parte del trattato dedicata ai principi generali dell'UE. L'articolo 16 crea anche una nuova base giuridica, conferendo all'UE la competenza a legiferare in materia di protezione dei dati. Si tratta di uno sviluppo importante, dal momento che inizialmente la

legislazione dell'UE in materia di protezione dei dati, segnatamente la direttiva sulla tutela dei dati, si fondava sulla base giuridica del mercato interno e sulla necessità di ravvicinare le legislazioni nazionali per non ostacolare la libera cir- colazione dei dati nell'UE. L'articolo 16 del TFUE fornisce ormai una base giuri- dica indipendente, per un approccio moderno e globale alla protezione dei dati, applicabile a tutte le questioni di competenza dell'UE, compresa la coopera- zione di polizia e giudiziaria in materia penale. L'articolo 16 del TFUE afferma altresì che l'osservanza delle norme di protezione dei dati adottate in confor- mità del medesimo sono soggette al controllo di autorità di sorveglianza indi- pendenti. L'articolo 16 è servito da base giuridica per l'adozione della riforma globale delle norme in materia di protezione dei dati nel 2016, vale a dire, il regolamento generale sulla protezione dei dati e la direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali (cfr. infra).

Il regolamento generale sulla protezione dei dati

Dal 1995 al maggio 2018 il principale strumento giuridico dell'UE in materia di protezione dei dati era costituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circo- lazione di tali dati (direttiva sulla

tutela dei dati)[29]. È stato adottato nel 1995, in un momento in cui diversi Stati membri avevano già adottato leggi nazio- nali in materia di protezione dei dati[30] e sorgeva dalla necessità di armoniz- zare tali leggi, per garantire un livello elevato di protezione e il libero flusso di dati personali tra i diversi Stati membri. La libera circolazione delle merci, dei capitali, dei servizi e delle persone nel mercato interno ha richiesto la libera circolazione dei dati, che non poteva essere realizzata se gli Stati membri non avessero potuto contare su un livello elevato e uniforme di protezione dei dati.

La direttiva sulla tutela dei dati rifletteva i principi di protezione dei dati già contemplati dalle legislazioni nazionali e dalla Convenzione n. 108, spesso ampliandoli. Essa si avvaleva della possibilità, prevista dall'articolo 11 della

Convenzione n. 108, di prevedere ulteriori strumenti di tutela. In particolare, l'introduzione nella direttiva di autorità di controllo indipendenti come stru- mento per migliorare l'osservanza delle norme sulla protezione dei dati ha dimostrato di contribuire in modo significativo all'effettivo funzionamento del diritto europeo in materia di protezione dei dati. Di conseguenza, questa caratteristica è stata ripresa nel diritto del CdE nel 2001 attraverso il Protocollo addizionale alla Convenzione n. 108. Questo illustra la stretta interazione e la reciproca influenza positiva tra i due strumenti nel corso degli anni.

La direttiva sulla tutela dei dati ha istituito nell'UE un sistema di protezione dei dati dettagliato e completo. Tuttavia, conformemente al sistema giuridico dell'UE, le direttive non si applicano direttamente e devono essere recepite nel diritto nazionale degli Stati membri. Inevitabilmente, gli Stati membri dispon- gono di un margine discrezionale nel recepire le disposizioni della direttiva. Sebbene l'intento della direttiva fosse di prevedere un'armonizzazione com- pleta[31] (e un livello di protezione totale), in pratica essa è stata recepita in modo diverso nei vari Stati membri. Ciò ha portato alla creazione di norme diversifi- cate in materia di protezione dei dati nell'UE e a interpretazioni diverse delle definizioni e delle norme nelle legislazioni nazionali. Anche i livelli di attuazione e la severità delle sanzioni differivano nei

vari Stati membri. Infine, dall'elabo- razione della direttiva, a metà degli anni '90, nelle tecnologie dell'informazione sono intervenuti cambiamenti significativi. L'insieme di questi motivi è all'ori- gine della riforma della legislazione dell'UE in materia di protezione dei dati.

La riforma ha portato all'adozione del regolamento generale sulla protezione dei dati nell'aprile 2016, dopo anni di accese discussioni. I dibattiti sulla neces- sità di modernizzare le norme dell'UE in materia di protezione dei dati hanno avuto inizio nel 2009, quando la Commissione ha effettuato una consultazione pubblica sul futuro quadro giuridico riguardante il diritto fondamentale alla pro- tezione dei dati personali. La proposta di regolamento è stata pubblicata dalla Commissione nel gennaio 2012, avviando un lungo iter legislativo di negozia- zione tra il Parlamento europeo e il Consiglio dell'UE. Dopo l'adozione, il rego- lamento generale sulla protezione dei dati prevedeva un periodo di transizione di due anni. È diventato pienamente applicabile il 25 maggio 2018, quando è stata abrogata la direttiva sulla tutela dei dati.

L’adozione del regolamento generale sulla protezione dei dati nel 2016 ha modernizzato la legislazione dell’UE in materia di protezione dei dati, renden- dola idonea a proteggere i diritti fondamentali nell’ambito delle sfide econo- miche e sociali dell’era digitale. Il RGPD preserva e sviluppa i principi e i diritti fondamentali dell’interessato, previsti dalla direttiva sulla tutela dei dati. Inol- tre, esso ha introdotto nuovi obblighi, che richiedono alle organizzazioni di attuare la protezione dei dati fin dalla progettazione e la protezione dei dati per impostazione predefinita; nominare un responsabile della protezione dei dati in determinate circostanze; rispettare un nuovo diritto alla portabilità dei dati e rispettare il principio di responsabilizzazione. In forza del diritto dell’UE, i regolamenti sono applicabili direttamente e non richiedono attuazione a livello nazionale. Il regolamento generale sulla protezione dei dati prevede pertanto un unico insieme di norme in materia di protezione di dati a livello dell’UE. Que- sto crea norme coerenti in materia di protezione dei dati in tutta l’UE, realiz- zando condizioni di certezza del diritto delle quali possono beneficiare opera- tori economici e individui in qualità di «interessati».

Nondimeno, anche se il regolamento generale sulla protezione dei dati è diret- tamente applicabile, gli Stati membri sono tenuti ad aggiornare le legislazioni nazionali vigenti in materia di protezione dei dati per allinearsi integralmente con il regolamento prevedendo al contempo, al

considerando 10, un margine di discrezionalità per disposizioni specifiche. Le principali norme e principi enun- ciati nel regolamento e i solidi diritti che accorda alle persone, costituiscono una parte importante del manuale e sono presentati nei capitoli seguenti. Il regolamento contiene norme approfondite sull'ambito di applicazione territo- riale. Esso si applica alle imprese stabilite nell'UE nonché ai titolari del trat- tamento e ai responsabili del trattamento non stabiliti nell'UE che offrono prodotti o servizi agli interessati nel territorio dell'UE o ne controllano il com- portamento. Dal momento che diverse imprese tecnologiche oltremare dispon- gono di una quota di mercato importante nel mercato europeo e milioni di clienti nell'UE, assoggettare tali organizzazioni alla legislazione dell'UE in mate- ria di protezione dei dati è importante per garantire la tutela delle persone e assicurare la parità di condizioni.

Protezione dei dati nel settore dell'applicazione della legge:
la direttiva 2016/680

L'abrogata direttiva sulla tutela dei dati prevedeva un regime globale di prote- zione dei dati. Tale regime è stato ora ulteriormente migliorato con l'adozione

del regolamento generale sulla protezione dei dati. Pur avendo portata globale, l'ambito di applicazione dell'abrogata direttiva sulla tutela dei dati era limitato alle attività nel mercato interno e alle attività delle autorità pubbliche diverse dall'applicazione della legge. Per conseguire la chiarezza e l'equilibrio neces- sari tra la protezione dei dati e altri interessi legittimi e affrontare le sfide par- ticolarmente pertinenti in settori specifici, era quindi necessaria l'adozione di appositi strumenti. È questo il caso delle norme che disciplinano il trattamento dei dati personali a opera delle autorità preposte all'applicazione della legge.

Il primo strumento giuridico dell'UE a disciplinare tale questione è stata la deci- sione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. Le sue disposizioni erano applicabili solo allo scambio tra Stati membri di dati personali nell'ambito delle attività giudiziarie e di polizia. Il trattamento dei dati personali a livello nazionale da parte delle autorità preposte all'applicazione della legge era escluso dal suo ambito di applicazione.

La direttiva 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o ese- cuzione di sanzioni

penali, nonché alla libera circolazione di tali dati[32], deno- minata direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, ha posto rimedio a tale situazione. Adottata contempora- neamente al regolamento generale sulla protezione dei dati, la direttiva ha abrogato la decisione quadro 2008/977/GAI, istituendo un regime globale di protezione dei dati personali nell’ambito dell’applicazione della legge, rico- noscendo al contempo le peculiarità del trat tamento dei dati relativo alla sicurezza pubblica. Mentre il regolamento generale sulla protezione dei dati stabilisce norme generali volte a proteggere le persone in relazione al trat- tamento dei loro dati personali e a garantire la libera circolazione di tali dati all’interno dell’UE, la direttiva stabilisce norme specifiche per la protezione dei dati nei settori della cooperazione giudiziaria in materia penale e della coope- razione di polizia. Qualora un’autorità competente tratti dati personali a fini di prevenzione, indagine, accertamento o perseguimento di reati, si applicherà la direttiva 2016/680. Qualora le autorità competenti trattino dati personali per

finalità diverse da quelle sopra menzionate, si applicherà il regime generale ai sensi del regolamento generale sulla protezione dei dati. A differenza del suo predecessore (la decisione quadro 2008/977/GAI del Consiglio), l'ambito di applicazione della direttiva 2016/680 si estende al trattamento dei dati per- sonali a livello nazionale, da parte delle autorità preposte all'applicazione della legge e non è limitata allo scambio di tali dati tra gli Stati membri. Inoltre, la direttiva si prefigge di realizzare un equilibrio tra i diritti delle persone e le fina- lità legittime del trattamento dei dati relativo alla sicurezza.

A tal fine, la direttiva sancisce il diritto alla protezione dei dati personali e i prin- cipi fondamentali che dovrebbero essere applicati al trattamento dei dati, basan- dosi rigorosamente sulle norme e sui principi sanciti dal regolamento generale sulla protezione dei dati. I diritti dei singoli e gli obblighi imposti ai titolari del trattamento – ad esempio in relazione alla sicurezza dei dati, alla protezione dei dati fin dalla progettazione e per impostazione predefinita nonché alle notifica- zioni di violazioni di dati – sono simili ai diritti e agli obblighi previsti dal rego- lamento generale sulla protezione dei dati. La direttiva prende inoltre in consi- derazione e cerca di affrontare le importanti sfide tecnologiche emergenti, che possono incidere in modo particolarmente oneroso sulle persone, come l'uso di tecniche di profilazione da parte delle autorità di

contrasto. In linea di principio, le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, devono essere vietate[33]. Inoltre, esse non devono basarsi su dati sensibili. Tali principi sono soggetti a talune eccezioni previste dalla direttiva. Inoltre, tale trattamento non deve portare alla discriminazione delle persone[34].

La direttiva contiene altresì disposizioni per garantire la responsabilità dei tito- lari del trattamento. Essi devono designare un responsabile della protezione dei dati per vigilare sull'osservanza delle norme in materia di protezione dei dati, informare e consigliare l'entità e i dipendenti che effettuano il trattamento circa gli obblighi loro incombenti, e cooperare con l'autorità di controllo. Il trat- tamento di dati personali nel settore della polizia e della giustizia penale è ora soggetto alla sorveglianza da parte di autorità di controllo indipendenti. Sia il regime giuridico generale di protezione dei dati sia il regime speciale di prote- zione dei dati in materia di applicazione della legge e questioni penali devono egualmente rispettare i requisiti della Carta dei diritti fondamentali dell'UE.

Il regime speciale per il trattamento dei dati nell'ambito della cooperazione giu- diziaria e di polizia, istituito dalla direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, è descritto in dettaglio nel capitolo 8.

La direttiva relativa alla vita privata e alle comunicazioni elettroniche

L'istituzione di norme specifiche per la protezione dei dati è stata giudicata necessaria anche nel settore delle comunicazioni elettroniche. Con lo sviluppo di Internet, della rete fissa e della telefonia mobile, era importante garantire il rispetto dei diritti degli utenti alla vita privata e alla riservatezza. La direttiva
2002/58/CE[35] relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche o direttiva e-privacy) contiene dispo- sizioni sulla sicurezza dei dati personali in tali reti, la notificazione delle viola- zioni dei dati personali e la riservatezza delle comunicazioni.

Per quanto riguarda la sicurezza, gli operatori dei servizi di comunicazione elettronica devono, tra l'altro, garantire che l'accesso ai dati personali sia limi- tato solo alle persone autorizzate e adottare misure atte a impedire che i dati personali siano distrutti, persi o accidentalmente danneggiati[36]. Nel

caso in cui esista un particolare rischio di violazione della sicurezza della rete pubblica di comunicazione, gli operatori devono informarne gli abbonati.[37] Se nonostante le misure di sicurezza attuate si verifica una violazione della sicurezza, gli ope- ratori devono notificare la violazione dei dati personali all'autorità nazionale competente incaricata dell'attuazione e dell'applicazione della direttiva. Gli operatori sono talvolta tenuti a notificare la violazione dei dati personali anche alle persone, segnatamente quando la violazione può avere conseguenze negative sui loro dati personali o sulla loro vita privata[38]. La riservatezza delle comunicazioni richiede che l'ascolto, la captazione, la memorizzazione o altre forme di sorveglianza o intercettazione delle comunicazioni e dei metadati siano, in linea di principio, vietate. La direttiva vieta altresì le comunicazioni indesiderate (alle quali viene spesso fatto riferimento come «spam»), a meno

che gli utenti abbiano prestato il loro consenso, e contiene disposizioni riguar- danti l'installazione di marcatori («cookies») su computer e dispositivi. Questi obblighi negativi fondamentali indicano chiaramente che la riservatezza delle comunicazioni è legata in modo significativo alla tutela del diritto al rispetto della vita privata sancito dall'articolo 7 della Carta e al diritto alla protezione dei dati personali sancito dall'articolo 8 della Carta.

Nel gennaio 2017, la Commissione ha pubblicato una proposta di regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunica- zioni elettroniche, inteso a sostituire la direttiva e- privacy. La riforma mira ad alli- neare le norme che disciplinano le comunicazioni elettroniche con il nuovo regime di protezione dei dati istituito a norma del regolamento generale sulla protezione dei dati. Il nuovo regolamento sarà direttamente applicabile in tutta l'UE; tutte le persone godranno dello stesso livello di protezione delle loro comunicazioni elettroniche, mentre gli operatori e le aziende del settore delle comunicazioni trarranno vantaggi dalla chiarezza e dalla certezza del diritto e dall'esistenza di un unico insieme di norme a livello dell'UE. Le norme proposte in materia di riser- vatezza delle comunicazioni elettroniche si applicheranno anche ai nuovi fornitori di servizi di comunicazione elettronica, che non rientrano nel campo di applica- zione della direttiva e-privacy. Quest'ultima riguardava solo i fornitori di servizi di telecomunicazione tradizionali.

Con la massiccia diffusione dell’uso di servizi quali Skype, WhatsApp, Facebook Messenger e Viber per inviare messaggi o effettuare chiamate, questi servizi over-the-top (servizi OTT) rientreranno ora nell’ambito di applicazione del regolamento e dovranno osservarne i requisiti in materia di protezione dei dati, vita privata e sicurezza. Al momento della pubblicazione di que- sto manuale, l’iter legislativo sulle norme di ePrivacy era ancora in corso.

Il regolamento n. 45/2001

Poiché la direttiva sulla tutela dei dati poteva essere applicata solo agli Stati membri dell’UE, si è avvertita l’esigenza di introdurre un ulteriore strumento giuridico per mettere in atto la protezione dei dati nell’ambito del trattamento dei dati personali da parte delle istituzioni e degli organismi dell’UE. Questo compito è svolto dal regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle isti- tuzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (regolamento sulla protezione dei dati da parte delle istituzioni dell’UE)[39].

Il regolamento n. 45/2001 segue rigorosamente i principi del regime generale dell'UE in materia di protezione dei dati e applica tali principi al trattamento dei dati effettuato dalle istituzioni e dagli organismi dell'UE nell'esercizio delle loro funzioni. Inoltre, esso istituisce un'autorità di controllo indipendente per moni- torare l'applicazione delle sue disposizioni, il Garante europeo della protezione dei dati (GEPD). Il GEPD è investito di poteri di controllo e ha il compito di sorve- gliare il trattamento dei dati personali nelle istituzioni e negli organismi dell'UE nonché di trattare i reclami e compiere i relativi accertamenti con riferimento a presunte violazioni delle norme in materia di protezione dei dati. Esso consiglia altresì le istituzioni e gli organismi dell'UE in ordine a qualsiasi argomento rela- tivo al trattamento dei dati personali, dalle nuove proposte legislative all'ado- zione di regolamentazioni interne relative al trattamento dei dati.

Nel gennaio 2017, la Commissione europea ha presentato la proposta di un nuovo regolamento relativo al trattamento dei dati da parte delle istituzioni dell'UE, che abrogherà l'attuale regolamento. Come nel caso della riforma della direttiva e-privacy, la riforma del regolamento n. 45/2001 sarà volta a moder- nizzare e allineare le proprie norme con il nuovo regime di protezione dei dati istituito a norma del regolamento generale sulla protezione dei dati.

Il ruolo della CGUE

La CGUE è competente a determinare se uno Stato membro abbia o meno adempiuto agli obblighi previsti dalla normativa dell’UE in materia di prote- zione dei dati e a interpretare la legislazione dell’UE per garantirne l’applica- zione efficace e uniforme in tutti gli Stati membri. Dall’adozione della direttiva sulla tutela dei dati nel 1995, si è accumulato un ampio corpus giurispruden- ziale, che chiarisce la portata e il significato dei principi di protezione dei dati e del diritto fondamentale alla protezione dei dati personali sancito dall’articolo
8 della Carta. Anche se la direttiva è stata abrogata ed è ora in vigore un nuovo strumento giuridico, il regolamento generale sulla protezione dei dati, tale giu- risprudenza preesistente rimane pertinente e valida ai fini dell’interpretazione e dell’applicazione dei principi dell’UE in materia di protezione dei dati, nella misura in cui i principi e i concetti fondamentali della direttiva sulla tutela dei dati sono stati mantenuti nel RGPD.

1.2. Limitazioni al diritto alla protezione dei dati personali

- Il diritto alla protezione dei dati personali non è un diritto assoluto e può essere limitato qualora sia necessario ai fini del perseguimento di un obiettivo di inte- resse generale o per proteggere i diritti e le libertà altrui.

- Le condizioni per limitare i diritti al rispetto della vita privata e alla protezione dei dati personali sono elencate nell'articolo 8 della CEDU e nell'articolo 52, para- grafo 1, della Carta. Queste sono state elaborate e interpretate attraverso la giu- risprudenza della Corte EDU e della CGUE.

- Nell'ambito del diritto del CdE in materia di protezione dei dati, il trattamento dei dati personali costituisce una legittima ingerenza nel diritto al rispetto alla vita privata e può essere attuato se:

- è conforme alla legge;

- persegue uno scopo legittimo;

- rispetta il contenuto essenziale dei diritti e delle libertà fondamentali;

- è necessaria e proporzionata in una società democratica per perseguire un obiettivo legittimo.

- L'ordinamento giuridico dell'UE prevede condizioni simili per quanto riguarda le limitazioni all'esercizio dei diritti fondamentali protetti dalla Carta. Qualsiasi limi- tazione di un diritto fondamentale, inclusa la protezione dei dati personali, può essere lecita soltanto se:

- è conforme alla legge;

- rispetta il contenuto essenziale del diritto;

- è necessaria nel rispetto del principio di proporzionalità;

- risponde a una finalità di interesse generale riconosciuta dall'UE o all'esi- genza di proteggere i diritti altrui.

Il diritto fondamentale alla protezione dei dati di carattere personale, ai sensi dell'articolo 8 della Carta, non appare come una prerogativa assoluta, «ma va considerato alla luce della sua funzione sociale»[40]. L'articolo 52, paragrafo 1,

della Carta riconosce, pertanto, che possono essere apportate limitazioni all'e- sercizio di diritti come quelli sanciti dagli articoli 7 e 8 della medesima, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà e, nel rispetto del principio di proporzionalità, siano neces- sarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere i diritti e le libertà altrui[41]. In modo analogo, nel sistema della CEDU, la protezione dei dati è garantita dall'articolo 8 e l'e- sercizio di tale diritto può essere limitato qualora sia necessario per perseguire un obiettivo legittimo. Questa sezione fa riferimento ai presupposti per l'in- gerenza nell'ambito della CEDU, come interpretato dalla giurisprudenza della Corte EDU, nonché alle condizioni per la legittimità delle limitazioni ai sensi dell'articolo 52 della Carta.

1.2.1. Requisiti che giustificano un'ingerenza ai sensi della CEDU

Il trattamento dei dati personali può costituire un'ingerenza nel diritto dell'inte- ressato al rispetto della vita privata, protetto dall'articolo 8 della CEDU[42]. Come spiegato in precedenza (cfr. sezioni 1.1.1 e 1.1.4.), contrariamente all'ordina- mento giuridico dell'UE, la CEDU non sancisce la protezione dei dati personali come diritto fondamentale distinto. Piuttosto, la protezione dei dati personali fa parte dei diritti tutelati dal diritto al rispetto della vita privata.

Pertanto, non tutte le operazioni che comportano il trattamento di dati personali possono rientrare nell'ambito di applicazione dell'articolo 8 della CEDU. Affinché l'arti- colo 8 sia applicabile, è necessario determinare in primo luogo se un interesse privato o la vita privata di una persona siano stati compromessi. Attraverso la sua giurisprudenza, la Corte EDU ha considerato la nozione di «vita privata» come un concetto ampio, in cui rientrano anche aspetti della vita professio- nale e il comportamento pubblico. Ha inoltre stabilito che la protezione dei dati personali costituisce una parte importante del diritto al rispetto della vita pri- vata. Nondimeno, nonostante l'interpretazione estensiva della nozione di vita privata, non tutti i tipi di trattamento comprometterebbero di per sé i diritti tutelati ai sensi dell'articolo 8.

Qualora la Corte EDU ritenga che l'operazione di trattamento in questione pregiudichi il diritto delle persone al rispetto della vita privata, esaminerà se

l'ingerenza sia giustificata. Il diritto al rispetto della vita privata non è un diritto assoluto, ma dev'essere contemperato e conciliato con altri diritti e interessi legittimi, siano essi di altre persone (interessi privati) o della società nel suo complesso (interessi pubblici).

Le condizioni cumulative che possono giustificare un'ingerenza sono illustrate di seguito.

Conformità alla legge

Secondo la giurisprudenza della Corte EDU, l'ingerenza avviene conformemente alla legge se si basa su una disposizione di diritto nazionale, che presenta talune caratteristiche. Il diritto dev'essere «accessibile alle persone interessate e prevedi- bile quanto ai suoi effetti»[43]. Una norma è prevedibile «se formulata in modo molto preciso per consentire all'interessato – avvalendosi, ove necessario, di consulenti esperti – di regolare il proprio comportamento»[44]. Inoltre, «[i]l grado di precisione della "legge" richiesto in tale contesto dipenderà dalla materia particolare»[45].

Esempi: nella causa *Rotaru c. Romania*[46], il ricorrente aveva fatto valere una violazione del suo diritto al rispetto della vita privata in ragione della detenzione e dell'utilizzo, da parte del servizio di intelligence romeno, di un file contenente

informazioni personali che lo riguardavano. La Corte EDU ha rilevato che la legge nazionale autorizzava la raccolta, la registrazione e l'archiviazione in fascicoli segreti di informazioni rilevanti per la sicurezza nazionale, ma non stabiliva limiti all'esercizio di tali poteri, che rimanevano a discrezione delle autorità. Il diritto nazionale non definiva, per esempio, il tipo d'informazioni che avrebbero potuto essere trattate, le categorie di

persone nei cui confronti si sarebbero potute adottare misure di sorveglianza, le circostanze in cui tali misure si sarebbero potute prendere o la proceduradada seguire. La Corte EDU ha pertanto concluso che il diritto nazionale non rispettava il requisito di prevedibilità ai sensi dell'articolo 8 della CEDU e che vi era stata una violazione di detto articolo.

Nella causa *Taylor-Sabori c. Regno Unito*[47], il ricorrente era stato sottoposto alla sorveglianza della polizia. Utilizzando un «clone» del cercapersone del ricorrente, la polizia era in grado di intercettare i messaggi inviatigli. Il ricorrente era stato arrestato e accusato di associazione a delinquere finalizzata al traffico di stupefacenti. Parte dell'impianto accusatorio a suo carico era costituito dai messaggi scritti contestuali del cercapersone, che erano stati trascritti dalla polizia. Tuttavia, all'epoca del processo del ricorrente, non vi era alcuna disposizione nella legge britannica che disciplinasse l'intercettazione delle comunicazioni trasmesse attraverso un sistema di telecomunicazioni privato. L'ingerenza nei suoi diritti non era avvenuta, quindi, «conformemente alla legge». La Corte EDU ha concluso che vi era stata violazione dell'articolo 8 della CEDU.

La causa *Vukota-Bojić c Svizzera*[48] riguardava la sorveglianza segreta di una richiedente

un’assicurazione sociale, da parte di investigatori privati commissionati dalla sua compagnia di assicurazione. La Corte EDU ha ritenuto che, sebbene la misura di sorveglianza oggetto del ricorso fosse stata ordinata da una compagnia di assicurazione privata, a tale società era stato riconosciuto dallo Stato il diritto di erogare prestazioni rientranti nell’assicurazione medica obbligatoria e di riscuotere premi assicurativi. Uno Stato non può esonerare se stesso dalle responsabilità previste dalla Convenzione, delegando i propri obblighi a enti privati o persone fisiche. Affinché l’ingerenza potesse essere «conforme alla legge», il diritto nazionale avrebbe dovuto fornire garanzie sufficienti contro l’abuso per ingerenza nei diritti di cui all’articolo 8 della CEDU. Nel caso in esame, la Corte EDU ha concluso che vi era stata violazione dell’articolo 8 della CEDU, in quanto il diritto nazionale non aveva indicato con sufficiente chiarezza la portata e le modalità dell’esercizio del potere discrezionale di esercitare una sorveglianza segreta su una persona assicurata, accordato a compagnie di assicurazione che agiscono in qualità di autorità pubbliche nelle controversie in materia

assicurativa. In particolare, esso non prevedeva garanzie sufficienti contro gli abusi.

Perseguimento di uno scopo legittimo

Lo scopo legittimo può essere costituito da uno degli interessi pubblici men- zionati o dalla protezione dei diritti e delle libertà altrui. Ai sensi dell'articolo 8, paragrafo 2, della CEDU, gli obiettivi legittimi che potrebbero giustificare un'in- gerenza sono gli interessi della sicurezza nazionale, la pubblica sicurezza o il benessere economico di un paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale e la protezione dei diritti e delle libertà altrui.

Esempio: nella causa *Peck c. Regno Unito*[49], il ricorrente aveva tentato il suicidio in strada tagliandosi i polsi, ignaro del fatto che una telecamera a circuito chiuso (CCTV) lo stesse filmando. La polizia, che stava guardando le telecamere CCTV, lo ha salvato e successivamente ha trasmesso i filmati a circuito chiuso ai media, che li hanno divulgati senza mascherare il volto del ricorrente. La Corte EDU ha rilevato l'assenza di motivi pertinenti o sufficienti che giustificassero la divulgazione diretta dei filmati da parte delle autorità al pubblico senza aver prima ottenuto il consenso del ricorrente o senza mascherarne l'identità. La

Corte ha concluso che vi era stata una violazione dell'articolo 8 della CEDU.

Necessità in una società democratica

La Corte EDU ha dichiarato che «la nozione di necessità comporta un'ingerenza basata su un'esigenza sociale imperativa e, in particolare, proporzionata al fine legittimo perseguito»[50]. Nel valutare se una misura sia necessaria per far fronte a un'esigenza sociale imperativa, la Corte EDU ne valuta la pertinenza e l'idoneità in relazione al fine perseguito. A tale scopo, essa può esaminare se l'ingerenza intenda risolvere un problema che, se non affrontato, potrebbe incidere negativamente sulla società, qualora esistano prove che l'ingerenza potrebbe attenuare tale effetto negativo, e quale più vasta visione ha la

società sul tema.[51] Ad esempio, la raccolta e l'archiviazione, da parte di servizi di sicurezza, di dati personali di individui specifici che si ritiene abbiano legami con movimenti terroristici, costituirebbero un'ingerenza nel diritto al rispetto della vita privata delle persone, che tuttavia soddisfa un'esigenza sociale seria e imperativa: la sicurezza nazionale e la lotta contro il terrorismo. Per soddi- sfare il criterio della necessità, l'ingerenza deve essere anche proporzionata. Nella giurisprudenza della Corte EDU, la proporzionalità è trattata nell'ambito della nozione di necessità. La proporzionalità richiede che un'ingerenza nei diritti sanciti dalla CEDU non vada oltre quanto è necessario per raggiungere la finalità legittima perseguita. Fattori importanti da considerare nel verificare il criterio di proporzionalità sono la portata dell'ingerenza, e in particolare il numero di persone interessate, e le garanzie o le condizioni poste in essere per limitarne la portata o gli effetti negativi sui diritti delle persone[52].

Esempio: nella causa *Khelili c. Svizzera*[53], la polizia, durante un controllo, ha rilevato che la ricorrente portava con sé biglietti da visita recanti la seguente dicitura: «Donna carina, piacente, sulla trentina avanzata, desidera incontrare un uomo per un drink o uscite saltuarie. Telefonare al n. [...]». La ricorrente aveva sostenuto che, a seguito di questa scoperta, la polizia aveva inserito il suo nome nei propri registri

classificandola come prostituta, professione che lei aveva costantemente negato di svolgere. La ricorrente aveva richiesto la cancellazione della parola «prostituta» dai registri informatici della polizia. La Corte EDU ha riconosciuto, in linea di principio, che la conservazione dei dati personali di un individuo sulla base del fatto che quella persona potrebbe commettere un altro reato può, in alcune circostanze, essere proporzionata. Tuttavia, nel caso della ricorrente, l'accusa di esercizio illecito della prostituzione sembrava troppo vaga e generica, non era suffragata da fatti concreti, poiché la donna non era mai stata condannata per esercizio illecito della prostituzione e non poteva quindi essere considerata compatibile con un'«esigenza sociale imperativa» ai sensi dell'articolo 8 della CEDU. Considerando la questione come un caso in cui sono le autorità a dovere dimostrare l'accuratezza dei dati conservati sulla ricorrente e alla luce della gravità dell'ingerenza nei diritti della stessa, la Corte EDU ha statuito che la

conservazione del termine «prostituta» nei fascicoli della polizia per anni non era necessaria in una società democratica. La Corte ha concluso che vi era stata violazione dell'articolo 8 della CEDU.

Esempio: nella causa *S. e Marper c. Regno Unito*[54], i due ricorrenti erano stati arrestati e accusati di reati penali. La polizia aveva rilevato le loro impronte digitali e campioni di DNA, come previsto dal *Police and Criminal Evidence Act* (legge sulla polizia e sulle prove di illeciti penali). I ricorrenti non erano mai stati condannati per i reati: uno era stato assolto in tribunale e, nel caso del secondo ricorrente, il procedimento penale a suo carico era stato interrotto. Cionondimeno, le loro impronte digitali, profili DNA e campioni di cellule erano custoditi e conservati dalla polizia in una banca dati, e la legislazione nazionale ne autorizzava la conservazione a tempo indeterminato. Mentre il Regno Unito aveva fatto valere l'utilità della conservazione ai fini dell'identificazione di autori di reati futuri, perseguendo così l'obiettivo legittimo di prevenzione e accertamento dei reati, la Corte EDU ha ritenuto ingiustificata l'ingerenza nel diritto dei ricorrenti al rispetto della vita privata. Essa ha ricordato che i principi fondamentali della protezione dei dati prevedono che la conservazione dei dati personali sia proporzionata rispetto alla finalità della raccolta e che i periodi di conservazione siano limitati. La Corte ha ammesso che estendere la banca dati per

includervi i profili DNA non solo dei condannati, ma anche di tutte le persone sospettate ma non condannate, avrebbe potuto contribuire all'accertamento e alla prevenzione dei reati nel Regno Unito. Tuttavia, è rimasta «sorpresa dal carattere generale ed indifferenziato con cui operail meccanismo di conservazione»[55].

Tenuto conto del patrimonio di informazioni genetiche e sulla salute contenute nei campioni di cellule, l'ingerenza nel diritto dei ricorrenti alla vita privata era particolarmente intrusiva. Impronte digitali e campioni potevano essere prelevati dalle persone arrestate e conservati nella banca dati della polizia a tempo indeterminato, indipendentemente dalla natura e dalla gravità del reato, e persino per reati minori non punibili con la reclusione. Inoltre, le possibilità per le persone assolte di ottenere la cancellazione dei propri dati dalla banca dati erano limitate. Infine, la Corte EDU ha tenuto in particolare considerazione il fatto che un ricorrente aveva undici anni al momento dell'arresto. Conservare i dati personali di un minore che non è stato condannato può essere particolarmente pregiudizievole, considerata

la sua vulnerabilità e l'importanza del suo sviluppo e della sua integrazione nella società[56]. La Corte ha ritenuto all'unanimità che la conservazione costituiva un'ingerenza sproporzionata nel diritto alla vita privata che non poteva essere considerata come necessaria in una società democratica.

Esempio: nella causa *Leander c. Svezia*[57], la Corte EDU ha stabilito che controllare in segreto le persone che fanno domanda d'impiego in posti di rilievo per la sicurezza nazionale non era, di per sé, in contrasto con il requisito di necessità in una società democratica. Le garanzie specifiche previste dal diritto nazionale a fini di tutela degli interessi dell'interessato – per esempio i controlli esercitati dal parlamento e dalla procura – hanno indotto la Corte EDU a concludere che il sistema di controllo svedese sul personale fosse conforme ai requisiti di cui all'articolo 8, paragrafo 2, della CEDU. In considerazione del suo ampio margine di discrezionalità, lo Stato convenuto aveva diritto di ritenere che, nel caso del ricorrente, gli interessi della sicurezza nazionale prevalessero su quelli individuali. La Corte EDU ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

1.2.2. Condizioni per la legittimità delle limitazioni ai sensi della Carta dei diritti fondamentali dell'UE

La struttura e la formulazione della Carta differiscono da quelle della CEDU. La Carta non utilizza la nozione di ingerenze nei diritti garantiti, ma contiene una disposi- zione sulle limitazioni dell'esercizio dei diritti e delle libertà da essa riconosciuti.

Ai sensi dell'articolo 52, paragrafo 1, le limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta e, di conseguenza, all'esercizio del diritto alla protezione dei dati personali, sono ammissibili solo se:

- sono previste dalla legge;

- rispettano il contenuto essenziale del diritto alla protezione dei dati;

- sono necessarie nel rispetto del principio di proporzionalità[58];

- rispondono a finalità d’interesse generale riconosciute dall’Unione o all’esi- genza di proteggere i diritti e le libertà altrui.

Dal momento che la protezione dei dati personali è un diritto fondamentale distinto e autonomo nell’ordinamento giuridico dell’UE, protetto ai sensi dell’ar- ticolo 8 della Carta, qualsiasi trattamento dei dati personali costituisce, di per sé, un’ingerenza in tale diritto. Il fatto che i dati personali in questione si rife- riscano alla vita privata di un individuo, che siano dati sensibili o che gli inte- ressati abbiano subito qualsivoglia disagio, è irrilevante. Per essere legittima, l’ingerenza deve soddisfare tutte le condizioni elencate nell’articolo 52, para- grafo 1, della CEDU.

Previsione per legge

Le limitazioni al diritto alla protezione dei dati personali devono essere previ- ste dalla legge. Tale requisito implica che le limitazioni devono fondarsi su una base giuridica che sia adeguatamente accessibile e prevedibile, oltre a essere formulate con precisione sufficiente per consentire alle persone di conoscere i propri obblighi e regolare la propria condotta. La base giuridica deve inoltre definire chiaramente la portata e le modalità dell’esercizio del potere da parte delle autorità competenti, per proteggere le persone da ingerenze arbitra- rie. Questa interpretazione è

simile al requisito per la «legittima ingerenza» ai sensi della giurisprudenza della Corte EDU[59], ed è stato sostenuto che il significato dell'espressione «prevista dalla legge» utilizzata nella Carta deve essere uguale a quello attribuito alla stessa in relazione alla CEDU[60]. La giuri- sprudenza della Corte EDU, e segnatamente la nozione di «qualità della legge» che essa ha elaborato nel corso degli anni, è una considerazione pertinente di cui la CGUE deve tenere conto nell'interpretare la portata dell'articolo 52, para- grafo 1, della Carta[61].

Rispetto del contenuto essenziale del diritto

Nell'ordinamento giuridico dell'UE, qualsiasi limitazione dei diritti fondamentali tutelati ai sensi della Carta deve rispettare il contenuto essenziale di tali diritti.

Ciò significa che limitazioni estese e invasive al punto di svuotare un diritto fondamentale del suo contenuto di base non possono essere giustificate. Se il contenuto essenziale del diritto è pregiudicato, la limitazione dev'essere considerata illegittima senza che occorra valutare ulteriormente se risponda a una finalità di interesse generale e soddisfi i requisiti della necessità e della proporzionalità.

Esempio: la causa *Schrems*[62] riguardava la tutela delle persone fisiche con riguardo al trasferimento dei loro dati personali verso paesi terzi, nella fattispecie, gli Stati Uniti. Il sig. Schrems, un cittadino austriaco che era stato iscritto a Facebook per diversi anni, aveva presentato denuncia presso l'autorità di protezione dei dati irlandese, sostenendo che i suoi dati personali erano stati trasferiti dalla controllata irlandese di Facebook verso Facebook Inc. e server situati negli Stati Uniti, dove erano stati trattati. Egli aveva sostenuto che, alla luce delle rivelazioni dell'informatore statunitense Edward Snowden nel 2013, concernenti le attività di sorveglianza dei servizi di intelligence degli Stati Uniti, il diritto e la prassi vigenti negli Stati Uniti non offrivano una protezione sufficiente dei dati personali trasferiti verso il territorio degli Stati Uniti. Snowden aveva rivelato che la National Security Agency intercettava direttamente i server di

aziende, come Facebook, e poteva leggere il contenuto di chat e messaggi privati.

I trasferimenti di dati verso gli Stati Uniti si basavano su una decisione di adeguatezza adottata dalla Commissione nel 2000, che consentiva trasferimenti verso le società statunitensi che autocertificavano la protezione da parte loro dei dati personali trasferiti dall'UE e il rispetto dei cosiddetti
«principi di approdo sicuro». Quando la causa è stata portata dinanzi alla CGUE, quest'ultima ha esaminato la validità della decisione della Commissione alla luce della Carta ricordando che la protezione dei diritti fondamentali nell'UE richiede che le deroghe e le restrizioni a tali diritti operino solo entro i limiti dello stretto necessario. La CGUE ha ritenuto che una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche «pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta». Il diritto sarebbe svuotato di significato qualora i pubblici poteri statunitensi fossero autorizzati ad accedere alle comunicazioni su base casuale, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente

riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate contro l'abuso di potere.

Inoltre, la CGUE ha osservato che «una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ot tenere la rettifica o la soppressione di tali dati» è incompatibile con il diritto fondamentale ad una tutela giurisdizionale effettiva (articolo 47 della Carta). Pertanto, la decisione «approdo sicuro» non aveva garantito un livello di protezione dei diritti fondamentali da parte degli USA sostanzialmente equivalente a quello garantito all'interno dell'UE in forza della direttiva letta alla luce della Carta. La CGUE ha di conseguenza invalidato la decisione[63].

Esempio: nella causa *Digital Rights Ireland*[64], la CGUE ha esaminato la compatibilità della direttiva 2006/24/CE (direttiva sulla conservazione dei dati) con gli articoli 7 e 8 della Carta. La direttiva obbligava i fornitori di servizi di comunicazione elettronica a conservare i dati relativi al traffico e i dati relativi all'ubicazione per un periodo non inferiore a sei mesi e non superiore a 24 mesi, e a permettere alle autorità nazionali competenti di accedere a tali dati a fini di prevenzione, indagine, accertamento e perseguimento di reati gravi. La direttiva non

permetteva la conservazione del contenuto delle comunicazioni elettroniche. La CGUE ha rilevato che i dati che i fornitori erano tenuti a conservare ai sensi della direttiva includevano i dati necessari per rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa, la data, l'ora e la durata di una comunicazione, il numero telefonico chiamante, i numeri chiamati nonché gli indirizzi IP. Questi dati,
«presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati».

Di conseguenza, la conservazione dei dati personali ai sensi della direttiva costituiva un'ingerenza particolarmente grave nei diritti alla vita privata e alla protezione dei dati personali. Tuttavia, la CGUE ha ritenuto che essa non pregiudicasse il contenuto essenziale di tali diritti. Per quanto riguarda il diritto alla vita privata, il suo contenuto essenziale non era compromesso, dal momento che la direttiva non permetteva di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tali. In modo analogo, non era compromesso il contenuto essenziale del diritto alla protezione dei dati personali, dal momento che la direttiva richiedeva ai fornitori di servizi di comunicazione elettronica di rispettare determinati principi di protezione dei dati e sicurezza dei dati e di applicare adeguate misure tecniche e organizzative in tal senso.

Necessità e proporzionalità

L'articolo 52, paragrafo 1, della Carta stabilisce che, nel rispetto del principio di proporzionalità, eventuali limitazioni all'esercizio dei diritti fondamentali e delle libertà riconosciuti dalla Carta possono essere apportate solo laddove siano necessarie.

Una limitazione può essere necessaria qualora occorra adottare misure ai fini del raggiungimento dell'obiettivo di interesse generale perseguito;

tuttavia, la necessità, così come interpretata dalla CGUE, implica anche che le misure adot- tate siano meno invasive rispetto ad altre opzioni finalizzate al raggiungimento del medesimo risultato. Per quanto riguarda le limitazioni dei diritti al rispetto della vita privata e alla protezione dei dati personali, la CGUE applica un rigido criterio di necessità, sostenendo che «deroghe e restrizioni interveng[o]no entro i limiti dello stretto necessario». Se una limitazione è considerata stretta- mente necessaria, occorre anche valutare se sia proporzionata.

Proporzionalità significa che i vantaggi risultanti dalla limitazione devono pre- valere sugli svantaggi causati dalla stessa in relazione all'esercizio dei diritti fondamentali in questione[65]. Per ridurre gli svantaggi e i rischi per il godimento dei diritti alla vita privata e alla protezione dei dati, è importante che le restri- zioni contengano garanzie adeguate.

Esempio: nella causa *Volker und Markus Schecke*[66], la CGUE ha concluso che, imponendo la pubblicazione di dati personali relativi ad ogni beneficiario dei sussidi di taluni fondi agricoli, senza operare distinzioni sulla base di criteri pertinenti come i periodi durante i quali esse hanno percepito simili aiuti, la frequenza o ancora il tipo e l'entità di questi ultimi, il Consiglio e la Commissione avevano superato i limiti imposti dal rispetto del principio di proporzionalità.

Pertanto, la CGUE ha ritenuto necessario dichiarare nulle alcune disposizioni del regolamento (CE) n. 1290/2005 del Consiglio nonché il regolamento n. 259/2008 nella sua interezza[67].

Esempio: nella causa *Digital Rights Ireland*,[68] la CGUE ha stabilito che l'ingerenza nel diritto alla vita privata causata dalla direttiva sulla conservazione dei dati non pregiudicava il contenuto essenziale di tale diritto, dal momento che vietava la conservazione del contenuto delle comunicazioni elettroniche. Tuttavia, essa ha concluso che la direttiva era incompatibile con gli articoli 7 e 8 della Carta, e l'ha dichiarata invalida. Dal momento che i dati relativi al traffico e all'ubicazione, aggregati e presi nel loro complesso, potevano essere analizzati e fornire un quadro dettagliato della vita privata delle persone, erano costitutivi di una grave ingerenza in tali diritti. La CGUE ha considerato che la direttiva

imponeva la conservazione di tutti i metadati riguardanti la telefonia fissa, la telefonia mobile, l'accesso a Internet, la posta elettronica su Internet nonché la telefonia via Internet. Pertanto essa concerneva tutti i mezzi di comunicazione elettronica il cui uso è estremamente diffuso nella vita quotidiana delle persone. In pratica, essa costituiva un'ingerenza che riguardava la totalità della popolazione europea. Tenuto conto della portata e della gravità di detta ingerenza, secondo la CGUE la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione poteva essere giustificata solo ai fini della lotta contro reati gravi. Inoltre, la direttiva non prevedeva criteri oggettivi per garantire che l'accesso da

parte delle autorità nazionali competenti ai dati conservati fosse limitato a quanto strettamente necessario. Oltre a ciò, essa non conteneva le condizioni sostanziali e procedurali a disciplina dell'accesso e dell'uso dei dati conservati da parte delle autorità nazionali competenti, che non erano subordinati ad un previo controllo da parte di un giudice o di un altro organismo indipendente.

La CGUE è giunta a una conclusione simile nelle cause riunite *Tele2 Sverige AB c. Post- och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson e a.*[69]. Tali cause concernevano la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione che riguardavano «tutti gli abbonati ed utenti iscritti e [...] tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati relativi al traffico», senza «differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito»[70]. Nella fattispecie, il fatto che una persona fosse o meno implicata, direttamente o indirettamente, in reati gravi, o il fatto che le sue comunicazioni fossero o meno rilevanti per la sicurezza nazionale, non costituivano una condizione per la conservazione dei loro dati. In assenza di una correlazione necessaria tra i dati conservati e una minaccia per la sicurezza pubblica o limitazioni aventi ad oggetto un periodo di tempo o una zona geografica, la CGUE ha concluso che la normativa nazionale travalicava i limiti dello stretto necessario ai fini della lotta contro la criminalità grave[71].

Un approccio simile, per quanto riguarda la necessità, è ripreso dal Garante europeo della protezione dei dati nella sua guida per la valutazione della necessità (*Necessity Toolkit*)[72]. La guida mira a fornire un aiuto nella valuta- zione della conformità delle misure proposte alla normativa dell'UE sulla prote- zione dei dati. Essa è stata concepita con lo scopo di rispondere meglio alle esi- genze dei responsabili politici e dei legislatori dell'UE nell'elaborazione o nello studio delle misure che prevedono il trattamento di dati personali e limitano il diritto alla protezione dei dati personali e altri diritti e libertà sanciti dalla Carta.

Finalità di interesse generale

Per essere giustificate, eventuali limitazioni all'esercizio dei diritti ricono- sciuti dalla Carta devono anche rispondere effettivamente a finalità di inte- resse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Per quanto riguarda la necessità di proteggere i diritti e le libertà altrui, il diritto alla protezione dei dati personali spesso interagisce con altri diritti fondamentali. La sezione 1.3 fornisce un'analisi dettagliata di tali interazioni. Per quanto riguarda gli obiettivi di interesse generale, questi inclu- dono gli obiettivi generali dell'UE sanciti dall'articolo 3 del trattato sull'Unione europea (TUE), quali la promozione della pace e del benessere dei suoi popoli, la giustizia e la protezione sociale, e la creazione di uno spazio di liber tà, sicurezza e giustizia in cui sia assicurata la libera circolazione delle persone, insieme a misure appropriate per quanto concerne la prevenzione della crimi- nalità e la lotta contro quest'ultima, come pure altri obiettivi e interessi tute- lati da disposizioni specifiche dei trattati[73]. Il regolamento generale sulla pro- tezione dei dati precisa ulteriormente l'articolo 52, paragrafo 1, della Carta al riguardo: L'articolo 23, paragrafo 1, del regolamento elenca una serie di obiet- tivi di interesse generale considerati legittimi per limitare i diritti delle persone, a condizione che la limitazione rispetti il contenuto essenziale del diritto alla protezione dei dati personali e sia necessaria e

proporzionata. La sicurezza nazionale e la difesa, la prevenzione di reati, la salvaguardia di importanti interessi economici e finanziari dell'UE o degli Stati membri, la sanità pub- blica e la sicurezza sociale sono alcuni tra gli obiettivi di interesse pubblico ivi menzionati.

Definire e spiegare in modo sufficientemente dettagliato l'obiettivo di inte- resse generale perseguito dalla limitazione è importante, poiché la necessità della limitazione sarà valutata in base a questo. Una descrizione chiara e det- tagliata dell'obiettivo della limitazione e delle misure proposte è essenziale per consentire di valutare se la limitazione sia necessaria[74]. L'obiettivo perse- guito nonché la necessità e proporzionalità della limitazione sono strettamente collegate.

Esempio: la causa *Schwarz c. Stadt Bochum*[75] riguardava limitazioni al diritto al rispetto della vita privata e al diritto alla tutela dei dati personali derivanti dal rilevamento e dalla conservazione di impronte digitali nel contesto del rilascio di passaporti da parte di autorità degli Stati membri[76]. Il ricorrente aveva chiesto il rilascio di un passaporto presso la Stadt Bochum, ma aveva rifiutato che gli venissero rilevate le impronte digitali; di conseguenza, la Stadt Bochum aveva respinto la sua domanda di passaporto. Egli aveva quindi proposto ricorso dinanzi a un giudice tedesco affinché gli venisse rilasciato un passaporto senza rilevare le sue impronte digitali. Il tribunale tedesco aveva rinviato la questione alla CGUE chiedendo se l'articolo 1, paragrafo 2, del regolamento n. 2252/2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri doveva essere considerato valido.

La CGUE ha sottolineato che le impronte digitali rientrano nella nozione di dati personali dato che contengono informazioni univoche su persone fisiche, che consentono di identificarle con precisione, mentre il prelievo e la conservazione delle impronte digitali rientrano nella nozione di trattamento. Detto trattamento, che è disciplinato dall'articolo 1, paragrafo 2, del regolamento n. 2252/2004, costituisce una

minaccia per i diritti al rispetto della vita privata e alla protezione dei dati personali[77]. Tuttavia, l'articolo 52, paragrafo 1, della Carta consente limitazioni all'esercizio di tali diritti, a condizione che siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e, conformemente al principio di proporzionalità, siano necessarie e rispondano effettivamente agli obiettivi di interesse generale riconosciuti dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Nella fattispecie, la CGUE ha innanzitutto rilevato che la limitazione derivante dal rilevamento e dalla conservazione di impronte digitali nel contesto del rilascio dei passaporti deve essere considerata prevista ex lege dato che tali operazioni sono previste dall'articolo 1, paragrafo 2, del regolamento n. 2252/2004. In secondo luogo, detto regolamento era finalizzato a prevenire la falsificazione dei passaporti e a impedirne un uso fraudolento. Pertanto, l'articolo 1, paragrafo 2, è diretto a impedire, tra l'altro, l'ingresso illegale di persone nel territorio dell'UE e, di conseguenza, persegue un

obiettivo di interesse generale riconosciuto dall'Unione. In terzo luogo, non risultava dagli elementi di cui la CGUE disponeva, e non era d'altra parte stato asserito, che le limitazioni apportate nella fattispecie all'esercizio di tali diritti non rispettavano il contenuto essenziale di siffatti diritti. In quarto luogo, la conservazione delle impronte digitali su un supporto di memorizzazione altamente securizzato, prevista da detta disposizione, implica una tecnica sofisticata. Tale conservazione può ridurre il rischio di falsificazione dei passaporti e agevolare il compito delle autorità incaricate di esaminare alle frontiere dell'UE la loro autenticità. Non è determinante che tale metodo sia totalmente affidabile. Sebbene esso non escluda completamente le accettazioni di persone non autorizzate, è sufficiente che riduca considerevolmente il rischio di tali accettazioni. Alla luce delle considerazioni che precedono, la CGUE ha constatato che il prelievo e la conservazione delle impronte digitali, previsti all'articolo 1, paragrafo 2, del regolamento n. 2252/2004, erano idonei a raggiungere le finalità perseguite da tale regolamento e, per estensione, l'obiettivo di impedire l'ingresso illegale di persone nel territorio dell'UE[78].

La CGUE ha quindi valutato se tale trattamento fosse necessario, rilevando che l'operazione in questione consisteva soltanto nel prendere

l’impronta di due dita, le quali, del resto, sono normalmente esposte alla vista altrui, di modo che non si tratta di un’operazione che riveste carattere intimo. Essa non comporta neppure un imbarazzo fisico o psichico particolare per l’interessato, come la fotografia del suo volto. Va inoltre osservato che l’unica reale alternativa al rilevamento delle impronte digitali richiamata nel corso del procedimento dinanzi alla CGUE consisteva nella cattura dell’immagine dell’iride dell’occhio. Nulla nel fascicolo sottoposto alla CGUE indicava che quest’ultimo procedimento fosse meno pregiudizievole ai diritti riconosciuti dagli articoli 7 e 8 della Carta rispetto al rilevamento delle impronte digitali. Inoltre, per quanto riguarda l’efficacia di questi due metodi, è pacifico che il livello di maturità tecnologica del metodo basato sul riconoscimento dell’iride non raggiunge il livello di quello basato sulle impronte digitali, il riconoscimento dell’iride è un procedimento notevolmente più oneroso, al momento attuale, di quello del confronto delle impronte digitali e, per questo motivo, meno idoneo ad un uso generalizzato. Di conseguenza, non era stata portata a conoscenza della CGUE l’esistenza di misure idonee a contribuire, in modo sufficientemente efficace, all’obiettivo di preservare i passaporti da un uso fraudolento, arrecando un pregiudizio minore ai diritti riconosciuti dagli

articoli 7 e 8 della Carta rispetto al pregiudizio arrecato dal metodo basato sulle impronte digitali[79].

La CGUE ha rilevato che l'articolo 4, paragrafo 3, del regolamento n. 2252/2004 precisa espressamente che le impronte digitali possono essere utilizzate soltanto allo scopo di verificare l'autenticità del passaporto e l'identità del suo titolare, mentre l'articolo 1, paragrafo 2, del regolamento prevede la conservazione delle impronte digitali soltanto all'interno del passaporto, il quale permane di esclusivo possesso del suo titolare. Pertanto, il regolamento non forniva un fondamento giuridico a una eventualecentralizzazione dei dati raccolti in base ad esso oppure all'impiego di questi ultimi a fini diversi da quello di impedire l'ingresso illegale di persone nel territorio dell'UE[80]. Alla luce dell'insieme delle considerazioni che precedono, la CGUE ha concluso che dall'esame della questione sollevata non sono emersi elementi atti ad inficiare la validità dell'articolo 1, paragrafo 2, del regolamento n. 2252/2004.

Relazione tra la Carta e la CEDU

Malgrado la formulazione diversa, le condizioni per la legittimità delle limi- tazioni dei diritti di cui all'articolo 52, paragrafo 1, della Carta ricordano l'ar- ticolo 8, paragrafo 2, della CEDU riguardante il

diritto al rispetto della vita privata. Nella loro giurisprudenza, la CGUE e la Corte EDU fanno spesso riferi- mento alle rispettive sentenze, nell’ambito del dialogo costante tra le due corti finalizzato a un’interpretazione coerente delle norme sulla protezione dei dati. L’articolo 52, paragrafo 3, della Carta statuisce che «[l]addove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell’Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta conven- zione». Tuttavia, l’articolo 8 della Carta non corrisponde direttamente a un articolo nella CEDU[81]. L’articolo 52, paragrafo 3 della Carta riguarda il conte- nuto e la portata dei diritti garantiti da ciascun ordinamento giuridico, piutto- sto che le condizioni per la loro limitazione. Tuttavia, in considerazione del più ampio contesto del dialogo e della cooperazione tra le due corti, la CGUE può

tenere in considerazione, nelle sue analisi, i criteri per la limitazione legittima ai sensi dell'articolo 8 della CEDU, come interpretati dalla Corte EDU. È possibile anche lo scenario opposto, in cui la Corte EDU può fare riferimento alle condi- zioni per la legittimità delle limitazioni ai sensi della Carta. In ogni caso, occorre altresì tenere conto del fatto che nella CEDU non esiste un perfetto equivalente dell'articolo 8 della Carta, il quale si riferisce alla protezione dei dati personali e, in particolare, ai diritti dell'interessato, ai motivi legittimi per il trattamento e al controllo di un'autorità indipendente. Alcune componenti dell'articolo 8 della Carta possono trovare fondamento nella giurisprudenza della Corte EDU, ela- borata ai sensi dell'articolo 8 della CEDU e della Convenzione n. 108[82]. Questo collegamento assicura un'ispirazione reciproca tra la CGUE e la Corte EDU in materia di protezione dei dati.

1.3. Interazione con altri diritti e interessi legittimi

- Il diritto alla protezione dei dati interagisce spesso con altri diritti, come la libertà di espressione e il diritto di ricevere e diffondere informazioni.

- Questa interazione è spesso ambivalente: mentre ci sono situazioni in cui il diritto alla

protezione dei dati personali è in conflitto con un diritto specifico, vi sono anche situazioni in cui il diritto alla protezione dei dati personali garantisce effet- tivamente il rispetto dello stesso diritto specifico. È questo il caso, ad esempio, della libertà di espressione, dato che il segreto professionale è un elemento del diritto al rispetto della vita privata.

• La necessità di proteggere i diritti e le libertà altrui è uno dei criteri utilizzati per valutare la limitazione legittima del diritto alla protezione dei dati personali.

• Quando sono in gioco diritti diversi, i tribunali devono trovare il giusto equilibrio per conciliarli.

• Il regolamento generale sulla protezione dei dati impone agli Stati membri di con- ciliare la protezione dei dati personali con il diritto alla libertà d'espressione e di informazione.

• Gli Stati membri possono anche adottare norme specifiche a livello nazionale per conciliare il diritto alla protezione dei dati personali con l'accesso del pubblico ai documenti ufficiali e l'obbligo al rispetto del segreto professionale.

Il diritto alla protezione dei dati personali non è un diritto assoluto; le condi- zioni per la legittimità delle limitazioni di questo diritto sono state illustrate in precedenza. Uno dei criteri per la legittimità della limitazione dei diritti rico- nosciuto sia dal diritto del CdE sia dal diritto dell'UE, è che l'ingerenza nella protezione dei dati deve essere necessaria per la tutela dei diritti e delle libertà altrui. Quando la protezione dei dati interagisce con altri diritti, sia la Corte EDU sia la CGUE hanno più volte ribadito che nell'applicazione e nell'interpretazione dell'articolo 8 della CEDU e dell'articolo 8 della Carta è necessario effettuare una ponderazione con altri diritti[83]. Alcuni esempi impor tanti illustreranno come è raggiunto tale equilibrio.

Oltre alla ponderazione effettuata da tali tribunali, se necessario gli Stati pos- sono adottare disposizioni per conciliare il diritto alla protezione dei dati per- sonali con altri diritti. Per questa ragione, il regolamento generale sulla prote- zione dei dati prevede la possibilità di deroghe nazionali in diversi settori.

Per quanto riguarda la libertà di espressione, il RGPD impone agli Stati membri di conciliare, per legge, «la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, ar tistica o letteraria»[84]. Gli Stati membri possono inoltre

adottare norme per conciliare la protezione dei dati con l'accesso del pubblico ai documenti ufficiali e il segreto professionale, tutelato quale forma del diritto al rispetto della vita privata.[85]

1.3.1. Libertà di espressione

Uno dei diritti che interagisce maggiormente con il diritto alla protezione dei dati è il diritto alla libertà di espressione.

La libertà di espressione è sancita dall'articolo 11 della Carta («Libertà di espres- sione e d'informazione»). Tale diritto include la «libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere

ingerenza da parte delle autorità pubbliche e senza limiti di frontiera». La libertà d'informazione ai sensi sia dell'articolo 11 della Carta sia dell'articolo 10 della CEDU tutela non solo il diritto a trasmettere, ma anche a *ricevere* informazioni.

Le limitazioni alla libertà di espressione devono rispettare i criteri di cui all'ar- ticolo 52, paragrafo 1 della Carta, sopra descritti. Inoltre, l'articolo 11 corri- sponde all'articolo 10 della CEDU. Ai sensi dell'articolo 52, paragrafo 3, della Carta, nella misura in cui prevede diritti corrispondenti a quelli garantiti dalla CEDU, «il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione». Le limitazioni che possono legittimamente essere imposte al diritto garantito dall'articolo 11 della Carta non possono pertanto andare oltre quelle previste all'articolo 10, paragrafo 2, della CEDU, vale a dire, devono essere previste dalla legge e necessarie in una società democratica «[...] alla protezione della reputazione o dei diritti altrui». Tali diritti includono, in particolare, il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali.

Il rapporto tra la protezione dei dati personali e la libertà di espressione è disci- plinato dall'articolo 85 del regolamento generale sulla protezione dei dati, dal titolo «Trattamento e libertà d'espressione e di informazione». In base a tale articolo, gli Stati membri devono conciliare la protezione dei dati

personali con il diritto alla libertà d'espressione e di informazione. In particolare, esenzioni e deroghe rispetto a capi specifici del regolamento generale sulla protezione dei dati sono previste a scopi giornalistici o di espressione accademica, artistica o letteraria, a condizione che siano necessarie per conciliare il diritto alla prote- zione dei dati personali e la libertà d'espressione e di informazione.

Esempio: nella causa *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*[86], alla CGUE è stato chiesto di definire la relazione tra la tutela dei dati personali e la libertà di stampa[87]. Essa doveva esaminare la divulgazione da parte di un'azienda, attraverso un servizio di SMS, di

dati fiscali di circa 1,2 milioni di persone fisiche, legittimamente ottenuti dalle autorità fiscali finlandesi. L'autorità di controllo per la protezione dei dati finlandese aveva emesso una decisione che imponeva all'azienda di cessare la divulgazione di tali dati. L'azienda aveva impugnato tale decisione dinanzi a un giudice nazionale, che ha chiesto chiarimenti alla CGUE in merito all'interpretazione della direttiva sulla tutela dei dati. In particolare, la CGUE doveva verificare se il trattamento di dati personali, messi a disposizione dalle autorità fiscali per consentire agli utenti di telefonia mobile di ricevere i dati fiscali relativi ad altre persone fisiche, dovesse essere considerato come un'attività esercitata esclusivamente a scopi giornalistici. Dopo avere concluso che le attività dell'azienda costituivano «trattamento di dati personali» ai sensi dell'articolo 3, paragrafo 1, della direttiva sulla tutela dei dati, la CGUE ha analizzato l'articolo 9 della direttiva (relativo al trattamento dei dati personali e alla libertà d'espressione). Essa ha in primo luogo evidenziato l'importanza del diritto alla libertà di espressione in tutte le società democratiche, rilevando che i concetti relativi a detta libertà, quali la nozione di giornalismo, dovrebbero essere interpretati in modo esteso. La Corte ha poi osservato che, per raggiungere un equilibrio tra i due diritti fondamentali, le deroghe e le limitazioni al diritto alla protezione dei dati devono applicarsi solo nella misura strettamente

necessaria. In tali circostanze, la CGUE ha stabilito che attività come quelle svolte dalle aziende in questione, relative ai dati provenienti da documenti che sono di dominio pubblico ai sensi della legislazione nazionale, possono essere qualificate come «attività giornalistiche» qualora siano dirette a divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione utilizzato. Essa ha anche stabilito che queste attività non sono riservate alle imprese operanti nel settore dei media e possono essere connesse a uno scopo di lucro. Tuttavia, relativamente al caso di specie, la CGUE ha rimesso la questione al giudice nazionale.

Lo stesso caso è stato esaminato anche dalla Corte EDU, dopo che il giudice nazionale aveva deciso, basandosi sugli orientamenti della CGUE, che il provvedimento dell'autorità di controllo di sospensione della pubblicazione di tutte le informazioni fiscali costituiva un'ingerenza giustificata nella libertà d'espressione dell'azienda. La Corte EDU ha confermato questo approccio[88]. Essa ha ritenuto che, malgrado la sussistenza di un'ingerenza nel diritto delle

aziende di comunicare informazioni, tale ingerenza era conforme alla legge, perseguiva uno scopo legittimo ed era necessaria in una società democratica.

La Corte ha richiamato i criteri giurisprudenziali che dovrebbero guidare le autorità nazionali e la Corte EDU stessa nel trovare un equilibrio tra la libertà di espressione e il diritto al rispetto della vita privata. Quando sono in gioco un discorso politico o un dibattito su una questione di interesse pubblico, rimane poco spazio per la limitazione del diritto di ricevere e comunicare informazioni, perché il pubblico ha il diritto di essere informato «e questo è un diritto fondamentale in una società democratica»[89]. Tuttavia, non si può ritenere che pubblicazioni miranti unicamente a soddisfare la curiosità di un pubblico in particolare riguardo alla vita privata di una persona contribuiscano a un dibattito di interesse pubblico. La deroga alle norme sulla protezione dei dati a scopi giornalistici è finalizzata a permettere ai giornalisti di accedere, raccogliere e trattare dati per poter svolgere la loro attività di giornalismo. Pertanto, sussisteva di fatto un interesse pubblico a fornire alle società richiedenti l'accesso alle grandi quantità di dati fiscali in questione e a consentire loro di acquisirli e trattarli. Per contro, la Corte ha rilevato che non vi era interesse pubblico nel diffondere detti dati grezzi in blocco tali e quali, e senza alcun apporto

analitico. Le informazioni di carattere fiscale avrebbero potuto permettere a cittadini curiosi di classificare le persone in base alla loro situazione economica e soddisfare la sete di informazioni del pubblico riguardo alla vita privata altrui. Ciò non poteva essere considerato un contributo a un dibattito di interesse pubblico.

Esempio: nella causa *Google Spain*,[90] la CGUE ha esaminato se Google fosse obbligata a eliminare dal suo elenco dei risultati di ricerca le informazioni obsolete concernenti le difficoltà finanziarie del ricorrente. Effettuando una ricerca nel motore di ricerca di Google utilizzando il nome del ricorrente, i risultati della ricerca fornivano collegamenti a vecchi articoli di giornale in cui era menzionato il suo collegamento a procedure fallimentari. Il ricorrente la riteneva una violazione dei suoi diritti al rispetto della vita privata e alla protezione dei dati personali, dal momento che il procedimento era stato definito diversi anni prima, rendendo irrilevante la menzione di tali riferimenti.

La CGUE ha innanzitutto chiarito che i motori di ricerca su Internet e i risultati di ricerca che forniscono dati personali possono stabilire un profilo dettagliato di una persona. In una società sempre più digitalizzata, il requisito dell'esattezza dei dati e il fatto che la loro pubblicazione non debba andare oltre quanto necessario, ad esempio per fornire informazioni al pubblico, sono fondamentali per garantire un livello elevato di protezione dei dati alle persone. Il «responsabile del trattamento in questione deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che tale trattamento soddisfi le prescrizioni» del diritto dell'UE, affinché le garanzie giuridiche previste sviluppino pienamente i loro effetti. Ciò significa che il diritto di ottenere la cancellazione dei propri dati personali quando il trattamento è obsoleto o non più necessario, riguarda anche i motori di ricerca, che sono stati considerati titolari del trattamento dei dati e non semplicemente responsabili del trattamento (cfr. sezione 2.3.1).

Nell'esaminare se Google fosse tenuta a eliminare i link collegati al ricorrente, la CGUE ha stabilito che, a determinate condizioni, le persone hanno il diritto di ottenere la cancellazione dei loro dati personali dai risultati di ricerca di un motore di ricerca su Internet. Questo diritto può essere invocato qualora le informazioni relative a una persona siano inesatte, inadeguate, non pertinenti o eccessive in

rapporto alle finalità del trattamento. La CGUE ha riconosciuto che tale diritto non è assoluto; esso deve essere ponderato con altri diritti, in particolare l'interesse e il diritto del grande pubblico ad avere accesso alle informazioni. Ogni richiesta di cancellazione deve essere valutata caso per caso, al fine di raggiungere un equilibrio tra i diritti fondamentali alla protezione dei dati personali e della vita privata dell'interessato, da un lato, e gli interessi legittimi di tutti gli utenti di Internet dall'altro. La CGUE ha fornito indicazioni sui fattori da considerare in materia di contemperamento. La natura dell'informazione di cui trattasi è un fattore particolarmente importante. Se le informazioni sono da considerare sensibili rispetto alla vita privata della persona e non vi è alcun interesse pubblico alla disponibilità dell'informazione, la protezione dei dati e della vita privata prevarrebbero sul diritto del pubblico generale di avere accesso all'informazione. Al contrario, ove risulti che l'interessato è una figura pubblica o che l'informazione è di natura tale da giustificarne la messa a disposizione del grande pubblico, l'ingerenza nei diritti fondamentali alla protezione dei dati e alla vita privata è giustificata.

A seguito della sentenza, il Gruppo di lavoro articolo 29 ha adottato linee guida per l'attuazione della sentenza della CGUE. Le linee guida includono un

elenco di criteri comuni a uso delle autorità di controllo nella loro attività di gestione di reclami relativi a richieste di cancellazione da parte delle persone e per fornire a tali autorità un orientamento in materia di contemperamento dei diritti[91].

Per quanto riguarda la conciliazione del diritto alla protezione dei dati con il diritto alla libertà di espressione, la Corte EDU ha emesso diverse sentenze cardine.

Esempio: nella causa *Axel Springer AG c. Germania*[92], la Corte EDU ha stabilito che un provvedimento che vietava a un'azienda di pubblicare un articolo riguardante l'arresto e la condanna di un noto attore violava l'articolo 10 della CEDU. La Corte EDU ha ribadito i criteri da considerare in materia di contemperamento del diritto alla libertà di espressione con il diritto al rispetto della vita privata, stabiliti nella propria giurisprudenza:

- se il fatto pubblicato dall'articolo in questione rivesta un interesse generale,

- se l'interessato sia un personaggio pubblico,

- in che modo l'informazione sia stata ottenuta e se sia affidabile.

La Corte EDU ha constatato che l’arresto e la condanna dell’attore erano un fatto giudiziario pubblico e quindi di interesse pubblico; che l’attore era sufficientemente noto per figurare quale personaggio pubblico, che l’informazione era stata fornita dall’ufficio della procura e l’esattezza delle informazioni non era oggetto di contenzioso tra le parti. Pertanto, le restrizioni alla pubblicazione imposte al giornale non erano state ragionevolmente proporzionate allo scopo legittimo di proteggere la vita privata del ricorrente. La Corte ha concluso che vi era stata una violazione dell’articolo 10 della CEDU.

Esempio: la causa *Coudec e Hachette Filipacchi Associés c. Francia*[93] riguardava la pubblicazione, da parte di un settimanale francese, di un'intervista con la sig.ra Coste, la quale sosteneva che il principe Alberto di Monaco era il padre di suo figlio. L'intervista descriveva anche la relazione tra la sig.ra Coste e il principe e il modo in cui quest'ultimo aveva reagito alla nascita del bambino, ed era accompagnata da fotografie del principe insieme al bambino. Il principe Alberto aveva intentato una causa nei confronti della casa editrice, per violazione del suo diritto alla protezione della vita privata. I tribunali francesi avevano concluso che la pubblicazione dell'articolo aveva causato danni irreversibili al principe Alberto e aveva condannato la casa editrice al risarcimento dei danni e alla pubblicazione dei dettagli della sentenza sulla pagina di copertina della rivista.

Gli editori della rivista avevano adito la Corte EDU, sostenendo che la sentenza dei tribunali francesi aveva interferito ingiustificatamente con il loro diritto alla libertà di espressione. La Corte EDU doveva contemperare il diritto del principe Alberto al rispetto della vita privata, con il diritto di espressione dell'editore e il diritto del grande pubblico di ottenere le informazioni. Il diritto della sig.ra Coste di condividere la propria storia con il pubblico e l'interesse del bambino al

riconoscimento ufficiale della relazione padre-figlio erano altrettante importanti considerazioni.

La Corte EDU ha stabilito che la pubblicazione dell'intervista costituiva un'ingerenza nella vita privata del principe e ha in seguito esaminato se tale ingerenza fosse necessaria. Essa ha stabilito che la pubblicazione riguardava un personaggio pubblico e una questione di interesse pubblico, dal momento che i cittadini di Monaco avevano interesse a conoscere l'esistenza di un figlio del principe, in quanto il futuro di una monarchia ereditaria è «intrinsecamente legato all'esistenza di discendenti» e quindi costituisce una questione oggetto di interesse per il pubblico[94]. La Corte ha altresì osservato che l'articolo aveva permesso alla sig.ra Coste e a suo figlio di esercitare il diritto alla libertà di espressione. I giudici nazionali non avevano tenuto sufficientemente conto dei principi e dei criteri elaborati dalla giurisprudenza della Corte EDU in materia di contemperamento del diritto al rispetto della vita privata e del diritto alla libertà di espressione. Essa ha concluso che la Francia aveva violato l'articolo 10 della CEDU.

Nella giurisprudenza della Corte EDU, uno dei criteri fondamentali per quanto riguarda la conciliazione di questi diritti è quello di stabilire se l'espressione in questione contribuisca o meno a un dibattito d'interesse pubblico generale.

Esempio: nella causa *Mosley c. Regno Unito*[95], un settimanale nazionale aveva pubblicato fotografie private del ricorrente, una figura nota, che in seguito aveva intentato una causa civile avverso l'editore, ottenendo il risarcimento dei danni. Malgrado la compensazione pecuniaria, il ricorrente aveva addotto di essere vittima di una violazione del suo diritto alla vita privata, dal momento che gli era stata negata la possibilità di chiedere un provvedimento inibitorio prima della pubblicazione delle foto in questione, a causa della mancanza di un obbligo giuridico di notifica preliminare per il quotidiano.

La Corte EDU ha osservato che, sebbene la divulgazione di tale materiale avesse generalmente finalità d'intrattenimento e non d'informazione, indubbiamente godeva della protezione prevista dall'articolo 10 della CEDU, sul quale potrebbero prevalere le prescrizioni dell'articolo 8 della CEDU in caso di informazione di natura intima e privata e di divulgazione senza alcun interesse pubblico. Tuttavia, particolare attenzione si imponeva in sede di esame delle restrizioni che

potrebbero costituire una forma di censura prima della pubblicazione. Per quanto riguarda l'eventuale effetto dissuasivo che insorgerebbe in caso di obbligo di notifica preliminare, i dubbi sulla sua efficacia e l'ampio margine di apprezzamento in quel settore, la Corte EDU ha concluso che l'esistenza di un obbligo di notifica preliminare vincolante non era richiesta ai sensi dell'articolo 8. Di conseguenza, la Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8.

Esempio: nella causa *Bohlen c. Germania*[96], il ricorrente, un noto cantante e produttore artistico, aveva pubblicato un libro autobiografico e, successivamente, era stato obbligato a rimuovere alcuni estratti in seguito a decisioni giudiziali. La storia aveva avuto ampia copertura da parte dei media nazionali e una società di tabacchi aveva lanciato una campagna pubblicitaria umoristica che faceva riferimento a questo aneddoto, utilizzando il nome proprio del ricorrente senza il suo consenso. Il ricorrente aveva invano chiesto

il risarcimento dei danni alla società di tabacchi, lamentando una violazione dei suoi diritti ai sensi dell'articolo 8 della CEDU. La Corte EDU ha ribadito i criteri che guidano la conciliazione del diritto al rispetto della vita privata e il diritto alla libertà di espressione e ha statuito che non vi era violazione dell'articolo 8. Il ricorrente era un personaggio pubblico e la pubblicità non faceva riferimento ai dettagli della sua vita privata, ma a un evento pubblico che era già stato coperto dai media e formava parte di un dibattito pubblico. Inoltre, la pubblicità aveva carattere umoristico e non presentava alcun contenuto degradante o negativo per il ricorrente.

Esempio: nella causa *Biriuk c. Lituania*[97], la ricorrente aveva sostenuto dinanzi alla Corte EDU che la Lituania non aveva rispettato l'obbligo di garantire il rispetto del suo diritto alla vita privata in quanto, sebbene un importante giornale avesse commesso una grave violazione della sua vita privata, i giudici nazionali che avevano esaminato il caso le avevano corrisposto una somma irrisoria a titolo di risarcimento dei danni patrimoniali. Nell'aggiudicare i danni morali, i giudici nazionali avevano applicato le disposizioni del diritto nazionale relativo alla fornitura di informazioni al pubblico, che fissava un massimale basso per il risarcimento di danni morali causati dalla diffusione illecita al pubblico da parte dei media di informazioni riguardanti la vita privata di

una persona. La controversia era stata originata dalla pubblicazione, da parte del più importante quotidiano lituano, di un articolo in prima pagina, che riportava la sieropositività della ricorrente. L'articolo criticava altresì il comportamento della ricorrente e metteva in discussione i suoi valori morali.

La Corte EDU ha ribadito che la protezione dei dati personali, e non ultimo dei dati sanitari, è di importanza fondamentale per il diritto al rispetto della vita privata sancito dalla CEDU. La riservatezza dei dati sanitari è particolarmente importante, poiché la divulgazione dei dati medici (nella fattispecie la condizione di sieropositività della ricorrente) può influenzare significativamente la vita privata e familiare di una persona, la sua situazione occupazionale e il suo inserimento nella società. La Corte ha attribuito particolare rilievo al fatto che, secondo l'articolo del giornale, il personale medico dell'ospedale aveva fornito informazioni sulla sieropositività della ricorrente, in manifesta violazione dell'obbligo al segreto medico. Di conseguenza, non vi era stata un'ingerenza legittima nel diritto alla vita privata della ricorrente.

L’articolo era stato pubblicato dalla stampa e anche la libertà di espressione è un diritto fondamentale ai sensi della CEDU. Tuttavia, nell’esaminare se la sussistenza di un interesse pubblico giustificasse la pubblicazione di questo tipo di informazione riguardante la ricorrente, la Corte ha ritenuto che lo scopo principale della pubblicazione fosse quello di aumentare le vendite del giornale soddisfacendo la curiosità dei lettori. Tale scopo non poteva essere considerato un contributo a un dibattito di interesse generale per la società. Trattandosi di un caso di «abuso oltraggioso della libertà di stampa», le pesanti limitazioni al risarcimento del danno e l’esiguo ammontare previsto per i danni morali dalla legislazione nazionale significavano che la Lituania non aveva adempiuto al suo obbligo positivo di proteggere il diritto della richiedente alla vita privata. La Corte EDU ha ritenuto che vi era stata una violazione dell’articolo 8 della CEDU.

Il diritto alla libertà di espressione e il diritto alla protezione dei dati personali non sono sempre in conflitto. Vi sono casi in cui la protezione effettiva dei dati personali garantisce la libertà di espressione.

Esempio: nella causa *Tele2 Sverige*, la CGUE ha stabilito che l’ingerenza determinata dalla direttiva 2006/24 (direttiva sulla conservazione dei dati) nei

diritti fondamentali sanciti dagli articoli 7 e 8 della Carta risultava essere
«di vasta portata e va considerata particolarmente grave. Inoltre, [...] il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate [...] la sensazione che la loro vita privata sia oggetto di costante sorveglianza». La CGUE ha altresì constatato che la conservazione generalizzata dei dati relativi al traffico e all'ubicazione potrebbe produrre un effetto sull'utilizzo delle comunicazioni elettroniche da parte degli utenti e «di conseguenza, sull'esercizio, da parte di questi ultimi, della loro libertà di espressione, garantita dall'articolo 11 della Carta»[98]. In tal senso, esigendo rigide garanzie affinché la conservazione dei dati non abbia luogo in modo generalizzato, le norme sulla protezione dei dati contribuiscono, in ultima analisi, all'esercizio della libertà di espressione.

Per quanto riguarda il diritto di ricevere informazioni, anch'esso parte della libertà di espressione, si osserva una crescente consapevolezza dell'importanza della trasparenza dei governi per il funzionamento di una società democratica. La trasparenza è un obiettivo di interesse generale che potrebbe, quindi, giustificare un'ingerenza nel diritto alla protezione dei dati, ove sia necessaria e proporzio- nata, come illustrato nella sezione 1.2. Di conseguenza, negli ultimi due decenni, il diritto di accedere ai documenti in possesso delle autorità pubbliche è stato riconosciuto come un importante diritto di ogni cittadino dell'UE nonché di ogni persona fisica o giuridica che risieda o abbia sede legale in uno Stato membro.

Ai sensi del diritto del CdE è possibile fare riferimento ai principi contemplati nella raccomandazione sull'accesso ai documenti ufficiali, che hanno ispirato i redattori della Convenzione sull'accesso ai documenti ufficiali (Convenzione n. 205)[99].

Ai sensi del diritto dell'UE il diritto di accesso ai documenti è garantito dal rego- lamento n. 1049/2001 relativo all'accesso del pubblico ai documenti del Parla- mento europeo, del Consiglio e della Commissione (regolamento sull'accesso ai documenti)[100]. L'articolo 42 della Carta e l'articolo 15, paragrafo 3, del TFUE hanno esteso tale diritto di accesso «ai documenti delle istituzioni, organi e orga- nismi dell'Unione, a prescindere dal loro supporto».

Questo diritto può entrare in conflitto con il diritto alla protezione dei dati qua- lora l’accesso a un documento riveli dati personali altrui. L’articolo 86 del rego- lamento generale sulla protezione dei dati prevede esplicitamente che i dati personali contenuti in documenti ufficiali in possesso di autorità e organismi pub- blici possono essere comunicati da tale autorità o organismo conformemente al diritto dell’Unione[101] o dello Stato membro al fine di conciliare l’accesso del pub- blico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del regolamento.

Le richieste di accesso ai documenti o alle informazioni in possesso delle autorità pubbliche possono quindi richiedere una conciliazione con il diritto alla prote- zione dei dati delle persone i cui dati sono contenuti nei documenti richiesti.

Esempio: nella causa *Volker und Markus Schecke e Hartmut Eifert c. Land Hessen*[102], la CGUE ha dovuto giudicare in merito alla proporzionalità della pubblicazione, prevista dalla normativa dell’UE, del nome dei beneficiari delle sovvenzioni agricole dell’Unione e degli importi da essi percepiti. La pubblicazione era volta a migliorare la trasparenza e contribuire al controllo pubblico dell’appropriatezza dell’uso dei fondi pubblici da parte dell’amministrazione. Diversi beneficiari avevano contestato la proporzionalità di tale pubblicazione.

La CGUE, pur rilevando che il diritto alla protezione dei dati non è assoluto, ha sostenuto che la pubblicazione su un sito Internet dei dati contenenti i nominativi dei beneficiari di due fondi per gli aiuti agricoli dell’UE e gli importi precisi percepiti costituisce un’ingerenza nella loro vita privata, in generale, e nella protezione dei dati personali, in particolare.

La CGUE ha ritenuto che tali ingerenze negli articoli 7 e 8 della Carta erano previste dalla legge e rispondevano a una finalità d’interesse generale riconosciuta dall’UE, segnatamente un rafforzamento della trasparenza sull’uso dei fondi dell’Unione. Tuttavia, la CGUE ha statuito che la pubblicazione dei nomi delle persone fisiche beneficiarie di

aiuti agricoli dell'UE provenienti da questi due fondi e gli importi precisi percepiti costituiva una misura sproporzionata e non era giustificata in considerazione dell'articolo 52, paragrafo 1, della Carta. Essa ha riconosciuto l'importanza, in una società democratica, di tenere informati i contribuenti sull'utilizzo delle finanze pubbliche. Tuttavia, dal momento che «non può riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali»[103], le istituzioni dell'UE hanno dovuto soppesare l'interesse dell'Unione alla trasparenza con la limitazione dell'esercizio dei diritti alla vita privata e alla protezione dei dati che i beneficiari avevano subito in seguito alla pubblicazione.

La CGUE ha stabilito che le istituzioni dell'UE non avevano effettuato un contemperamento equilibrato, dal momento che erano concepibili misure che avrebbero determinato lesioni meno gravi dei diritti fondamentali delle persone, contribuendo nel contempo in maniera efficace all'obiettivo

di trasparenza perseguito dalla pubblicazione. Ad esempio, anziché una pubblicazione generale riguardante tutti i beneficiari, in cui sono forniti il nome e gli importi ricevuti da ciascuno, si potrebbe operare una distinzione sulla base di criteri pertinenti come i periodi durante i quali tali persone hanno percepito gli aiuti, la frequenza o il tipo e l'entità degli stessi[104]. La CGUE ha quindi dichiarato parzialmente nulla la legislazione dell'UE sulla pubblicazione delle informazioni relative ai beneficiari dei fondi agricoli europei.

Esempio: nella causa *Rechnungshof c. Österreichischer Rundfunk e a.*[105], la CGUE ha esaminato la compatibilità di alcuni aspetti della legislazione austriaca con il diritto dell'UE in materia di protezione dei dati. La normativa obbligava un organo statale alla raccolta e alla trasmissione dei dati sui redditi allo scopo di pubblicare i nomi e i redditi dei dipendenti di diversi enti pubblici in una relazione annuale messa a disposizione del grande pubblico. Alcune persone si erano rifiutate di comunicare i propri dati per motivi di protezione dei dati.

Nelle sue conclusioni, la CGUE ha invocato la protezione dei diritti fondamentali quale principio generale del diritto dell'UE e l'articolo 8 della CEDU, ricordando che all'epoca la Carta non era vincolante. Essa ha stabilito che la raccolta di dati relativi al reddito professionale di un

individuo, e in particolare la loro comunicazione a terzi, rientra nel campo di applicazione del diritto al rispetto della vita privata e costituisce una violazione di tale diritto. L'ingerenza avrebbe potuto essere giustificata se fosse stata prevista dalla legge, avesse perseguito una finalità legittima e fosse stata necessaria in una società democratica per la realizzazione di tale finalità. La CGUE ha osservato che la normativa austriaca perseguiva una finalità legittima, dal momento che il suo obiettivo era di mantenere le retribuzioni dei funzionari pubblici entro limiti ragionevoli; una considerazione che è legata anche al benessere economico del paese. Tuttavia, l'interesse dell'Austria a garantire un impiego ottimale delle finanze pubbliche doveva essere ponderato con la gravità dell'ingerenza nel diritto delle persone interessate al rispetto della loro vita privata.

Lasciando al giudice nazionale il compito di verificare se la pubblicazione dei dati riguardanti il reddito delle persone fisiche fosse necessaria e proporzionata alla finalità perseguita dalla normativa, la CGUE ha chiesto al giudice nazionale di esaminare se tale obiettivo non avrebbe potuto essere realizzato in modo ugualmente efficace con mezzi meno invasivi. Un esempio potrebbe essere la trasmissione dei dati personali ai soli organi di controllo e non al grande pubblico.

In casi successivi, è risultato evidente che la ponderazione tra la protezione dei dati e l'accesso ai documenti richiede un'analisi approfondita caso per caso. Nessun diritto può prevalere automaticamente sull'altro. La CGUE ha avuto la possibilità di interpretare il diritto di accesso a documenti contenenti dati per- sonali in due casi.

Esempio: nella causa *Commissione europea c. The Bavarian Lager*[106], la CGUE ha definito la portata della protezione dei dati personali nel contesto dell'accesso ai documenti delle istituzioni dell'UE e secondo il rapporto tra il regolamento n. 1049/2001 (regolamento sull'accesso ai documenti) e il regolamento n. 45/2001 (regolamento sulla protezione dei dati da parte delle istituzioni dell'UE). La società Bavarian Lager, fondata nel 1992, importa birra tedesca in bottiglia nel Regno Unito,

principalmente per locali pubblici e bar. Tuttavia, la società riscontrava difficoltà perché la legislazione britannica favoriva di fatto i produttori nazionali. In risposta alla denuncia della Bavarian Lager, la Commissione europea aveva avviato un procedimento contro il Regno Unito per mancato adempimento dei propri obblighi, che ha portato a modificare le disposizioni controverse e ad allinearle con il diritto dell'UE. La Bavarian Lager ha poi chiesto alla Commissione, fra gli altri documenti, una copia del verbale di una riunione cui avevano partecipato i rappresentanti della Commissione, le autorità britanniche e la *Confédération des Brasseurs du Marché Commun* (CBMC). La Commissione aveva accettato di divulgare alcuni documenti relativi alla riunione, cancellando tuttavia cinque nomi che figuravano a verbale, ossia due persone che si erano esplicitamente opposte alla divulgazione della loro identità e altre tre che la Commissione non riusciva a contattare. Con decisione del 18 marzo 2004, la Commissione aveva respinto una nuova domanda della Bavarian Lager volta a ottenere il verbale integrale della riunione, citando in particolare la protezione della

vita privata delle persone, come garantito dal regolamento sulla protezione dei dati da parte delle istituzioni dell'UE.

Non soddisfatta di tale decisione, la Bavarian Lager ha presentato ricorso dinanzi al Tribunale, il quale ha annullato la decisione della Commissione con sentenza dell'8 novembre 2007 (causa T-194/04, *The Bavarian Lager Co. Ltd c. Commissione delle Comunità europee*), ritenendo che l'inserimento dei soli nomi delle persone in questione nell'elenco di partecipanti alla riunione per conto dell'organismo che rappresentavano non costituiva un pregiudizio né un pericolo per la vita privata di tali persone.

Su ricorso della Commissione, la CGUE ha annullato la sentenza del Tribunale di primo grado, statuendo che il regolamento sull'accesso ai documenti prevede «un regime specifico e rafforzato di tutela di una persona i cui dati personali possano, eventualmente, essere comunicati al pubblico». Secondo la CGUE, nel caso di una domanda fondata sul regolamento sull'accesso ai documenti che sia diretta a ottenere l'accesso a documenti contenenti dati personali, sono integralmente applicabili le disposizioni del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE. La CGUE ha concluso quindi che la Commissione aveva legittimamente respinto la domanda di accesso al

verbale completo della riunione dell'ottobre 1996. In assenza del consenso dei cinque partecipanti a tale riunione, la Commissione, diffondendo una versione del documento controverso priva dei nomi in questione, aveva ottemperato sufficientemente al proprio obbligo di trasparenza.

Inoltre, secondo la CGUE, «dal momento che la Bavarian Lager non ha fornito alcuna motivazione espressa e legittima né alcun argomento convincente per dimostrare la necessità del trasferimento di questi dati personali, la Commissione non ha potuto soppesare i differenti interessi delle parti in causa. Essa non era neppure in grado di verificare se sussistevano ragioni per presumere che tale trasferimento avrebbe arrecato pregiudizio agli interessi legittimi delle persone coinvolte», come richiesto dal regolamento sulla protezione dei dati da parte delle istituzioni dell'UE.

Esempio: nella causa *ClientEarth e PAN Europe c. EFSA*[107], la CGUE ha esaminato se la decisione dell'Autorità europea per la sicurezza alimentare

(EFSA) di rifiutare ai ricorrenti l'accesso integrale ai documenti fosse necessaria per proteggere i diritti alla vita privata e alla protezione dei dati delle persone alle quali i documenti si riferivano. I documenti riguardavano un progetto di orientamento redatto da un gruppo di lavoro dell'EFSA in collaborazione con esperti esterni, concernente l'immissione in commercio di prodotti fitosanitari. In un primo tempo, l'EFSA aveva concesso ai ricorrenti un accesso parziale, negando l'accesso ad alcune versioni di lavoro del progetto di orientamento. Successivamente, aveva concesso l'accesso alla versione del progetto che conteneva osservazioni individuali degli esperti esterni. Essa aveva, tuttavia, occultato i nomi degli esperti, invocando l'articolo 4, paragrafo 1, lettera b), del regolamento n. 45/2001 sul trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE e la necessità di proteggere la vita privata degli esperti esterni. In primo grado, il Tribunale dell'UE ha accolto la decisione dell'EFSA.

Su ricorso dei ricorrenti, la CGUE ha annullato la sentenza di primo grado. Essa ha concluso che, nella fattispecie, il trasferimento dei dati personali era necessario per accer tare l'imparzialità di ciascun esper to esterno nell'adempimento della sua missione scientifica e per garantire la trasparenza del processo decisionale all'interno dell'EFSA. Secondo la CGUE, l'EFSA non aveva precisato in che modo la divulgazione dei nomi degli esperti esterni che

avevano presentato osservazioni specifiche sul progetto di orientamento avrebbe pregiudicato gli interessi legittimi degli esperti. Un'argomentazione generale secondo cui la divulgazione potrebbe comportare un potenziale pregiudizio per la vita privata non è sufficiente se non è supportata da altri elementi del caso di specie.

Secondo queste sentenze, l'ingerenza nel diritto alla protezione dei dati per quanto riguarda l'accesso ai documenti esige una ragione specifica e motivata. Il diritto di accesso ai documenti non può prevalere automaticamente sul diritto alla protezione dei dati[108].

Questo approccio è simile a quello adottato dalla Corte EDU in materia di vita privata e accesso ai documenti, come dimostra la seguente sentenza. Nella sen- tenza *Magyar Helsinki*, la Corte EDU ha stabilito che l'articolo 10 non conferisce

all’individuo un diritto di accesso alle informazioni detenute dalle autorità pub- bliche, né obbliga lo Stato a comunicare tali informazioni all’individuo. Tuttavia tale diritto o obbligazione potrebbe sorgere, in primo luogo, quando la divul- gazione delle informazioni è imposta da un provvedimento giudiziario divenuto esecutivo e, in secondo luogo, quando l’accesso all’informazione è strumen- tale rispetto all’esercizio da parte di una persona del proprio diritto alla libertà di espressione, in particolare la libertà di ricevere e comunicare informazioni, e quando il suo rifiuto costituirebbe un’ingerenza in tale diritto[109]. Se e in quale misura il rifiuto di concedere l’accesso alle informazioni costituisca un’ingerenza nella libertà di espressione di un richiedente, è una questione da valutare caso per caso e alla luce delle circostanze particolari, che comprendono: a) lo scopo della richiesta di informazioni, b) la natura delle informazioni richieste, c) il ruolo del richiedente e d) se le informazioni erano pronte e disponibili.

Esempio: nella causa *Magyar Helsinki Bizottság c. Ungheria*[110], la richiedente, una ONG attiva nel settore dei diritti umani, aveva chiesto informazioni alla polizia in relazione all’operato di difensori d’ufficio, per completare uno studio sul funzionamento del sistema dei difensori d’ufficio in Ungheria. La polizia aveva rifiutato di fornire le informazioni, adducendo che si trattava di dati

personali non soggetti a divulgazione. Applicando i criteri di cui sopra, la Corte EDU aveva constatato un'ingerenza nell'esercizio di un diritto tutelato ai sensi dell'articolo 10. Più precisamente, la richiedente intendeva esercitare il diritto di divulgare informazioni riguardanti una questione di interesse pubblico, aveva chiesto a tale scopo l'accesso alle informazioni e queste ultime erano necessarie per l'esercizio del diritto della ricorrente alla libertà di espressione. Le informazioni riguardanti la designazione di difensori d'ufficio erano di interesse per il pubblico. Non vi era ragione di dubitare che lo studio in questione contenesse informazioni che la richiedente aveva intenzione di comunicare al pubblico e che il pubblico aveva il diritto di ricevere. La Corte ha ritenuto quindi che l'accesso alle informazioni richieste era necessario alla richiedente per svolgere il suo compito. Infine, le informazioni erano pronte e disponibili.

La Corte EDU ha concluso che, nella fattispecie, il rifiuto di dare accesso alle informazioni aveva compromesso la sostanza stessa della libertà di ricevere

informazioni. Per giungere a questa conclusione, essa ha esaminato, in particolare, lo scopo della richiesta di informazioni e il suo contributo a un importante dibattito pubblico, la natura dell'informazione richiesta e se fosse di interesse pubblico, nonché il ruolo svolto nella società dalla richiedente nella fattispecie.

Nel ragionamento svolto dalla Corte, essa ha osservato che lo studio condotto dalla ONG riguardava il funzionamento della giustizia e il diritto a un'equa e pubblica udienza, che era un diritto di importanza fondamentale sancito dalla CEDU. Dal momento che le informazioni richieste non riguardavano dati al di fuori del dominio pubblico, i diritti degli interessati al rispetto della vita privata (i difensori d'ufficio) non sarebbero stati compromessi se la polizia avesse consentito alla richiedente l'accesso alle informazioni. Le informazioni richieste dalla ricorrente erano di natura statistica e si riferivano al numero di volte che i difensori d'ufficio erano stati designati per rappresentare un imputato in occasione di procedimenti penali pubblici.

Per la Corte, dal momento che lo studio era inteso a contribuire a un importante dibattito su una questione di interesse generale, qualsiasi limitazione alla pubblicazione proposta dall'ONG avrebbe dovuto essere sottoposta a un controllo minuzioso. Le informazioni di cui trattasi erano di interesse pubblico, dal momento che quest

’ultimo comprende le «questioni suscettibili di creare vive polemiche, che riguardano una problematica sociale importante, o che trattano un problema del quale il pubblico avrebbe interesse ad essere informato»[111]. Rientrerebbe pertanto certamente nell’interesse pubblico una discussione sull’amministrazione della giustizia e sull’equità dei processi, che era l’oggetto dello studio della ricorrente. Nel conciliare i diversi diritti in questione e applicando il principio di proporzionalità, la Corte EDU ha concluso che vi era stata una violazione ingiustificata dei diritti della ricorrente ai sensi dell’articolo 10 della CEDU.

1.3.2. Segreto professionale

Ai sensi del diritto nazionale, determinate comunicazioni possono essere sog- gette al vincolo del segreto professionale. Il segreto professionale può essere def inito come uno speciale dovere etico, che prevede un obbligo legale

inerente a determinate professioni e funzioni basate sulla fiducia. Le persone e le istituzioni che esercitano tali funzioni sono obbligate a non rivelare le infor- mazioni riservate ricevute nello svolgimento dei loro compiti. Il segreto profes- sionale si applica, in particolare, alla professione medica e al rapporto privile- giato tra avvocato e cliente, e molte giurisdizioni riconoscono anche un obbligo di segretezza professionale nel settore finanziario. Il segreto professionale non è un diritto fondamentale, ma è tutelato in quanto è una forma del diritto al rispetto della vita privata. Per esempio, la CGUE ha stabilito che, in alcuni casi,
«può essere infatti necessario vietare la divulgazione di talune informazioni qualificate come riservate, al fine di preservare il diritto fondamentale di un'im- presa al rispetto della vita privata, sancito all'articolo 8 della [...] CEDU e all'arti- colo 7 della Carta»[112]. La Corte EDU è stata anche chiamata a pronunciarsi sulla questione se le limitazioni al segreto professionale costituiscano una violazione dell'articolo 8 della CEDU, come illustrato negli esempi messi in evidenza.

Esempio: nella causa *Pruteanu c. Romania*[113], il ricorrente agiva in qualità di avvocato di una società commerciale, alla quale era stato interdetto il compimento di operazioni bancarie in seguito ad accuse di frode. Nel corso dello svolgimento dell'inchiesta, i tribunali rumeni avevano autorizzato

le autorità inquirenti a intercettare e registrare le conversazioni telefoniche di un socio dell'azienda per un certo periodo. Le registrazioni e le intercettazioni comprendevano le comunicazioni di quest'ultimo con il suo avvocato.

Il sig. Pruteanu aveva sostenuto che ciò costituiva un'ingerenza nel diritto al rispetto della sua vita privata e della sua corrispondenza. Nella sua sentenza, la Corte EDU ha evidenziato lo status e l'importanza del rapporto di un avvocato con il proprio cliente. L'intercettazione delle conversazioni di un avvocato con il proprio cliente violavano indubbiamente il segreto professionale, che era alla base della relazione tra le due persone. In questo caso, l'avvocato poteva lamentare anche un'ingerenza nel proprio diritto al rispetto della vita privata e della corrispondenza. La CJUE ha statuito che vi era stata una violazione dell'articolo 8 della CEDU.

Esempio: nella causa *Brito Ferrinho Bexiga Villa-Nova c. Portogallo*[114], la ricorrente, un avvocato, aveva rifiutato di divulgare i propri estratti conto personali alle autorità fiscali facendo valere il segreto professionale e il segreto bancario. La procura aveva aperto un'inchiesta per frode fiscale e chiesto l'autorizzazione a sospendere il segreto professionale. I tribunali nazionali avevano ordinato la sospensione delle norme sul segreto professionale e sul segreto bancario, ritenendo che l'interesse pubblico doveva prevalere sugli interessi privati della ricorrente.

Quando la causa è giunta dinanzi alla Corte EDU, quest'ultima ha stabilito che l'accesso agli estratti conto della ricorrente costituiva un'ingerenza nel suo diritto al rispetto del segreto professionale, che rientra nell'ambito della vita privata. L'ingerenza aveva una base giuridica, dal momento che si fondava sul codice di procedura penale, e perseguiva uno scopo legittimo. Tuttavia, esaminando la necessità e la proporzionalità dell'ingerenza, la Corte EDU ha sottolineato il fatto che il procedimento diretto ad eliminare la riservatezza si era svolto senza la partecipazione della ricorrente, e senza che quest'ultima ne fosse a conoscenza. La ricorrente non aveva, pertanto, potuto presentare le proprie argomentazioni. Inoltre, anche se il diritto nazionale prevedeva che l'associazione degli avvocati dovesse essere consultata in tali procedimenti, ciò non era avvenuto. Infine, la

ricorrente non aveva la possibilità di contestare efficacemente la revoca della riservatezza, né di presentare un ricorso tramite il quale opporsi alla misura. In ragione della mancanza di garanzie procedurali e di un controllo giurisdizionale effettivo sulla misura che sospendesse l'obbligo di riservatezza, la Corte EDU ha concluso che vi era stata violazione dell'articolo 8 della CEDU.

L'interazione tra il segreto professionale e la protezione dei dati è spesso ambi- valente. Da un lato, le norme e le garanzie in materia di protezione dei dati sta- bilite dalla legislazione contribuiscono a garantire il segreto professionale. Ad esempio, le norme che impongono ai titolari del trattamento e ai responsabili del trattamento di attuare rigorose misure di sicurezza dei dati sono finaliz- zate a evitare, tra l'altro, la perdita di riservatezza dei dati personali garantita dal segreto professionale. Inoltre, il regolamento generale sulla protezione dei dati dell'UE permette il trattamento dei dati sanitari, i quali costituiscono una categoria particolare di dati personali che meritano maggiore protezione, ma lo assoggetta all'esistenza di misure appropriate e specifiche a salvaguardia

dei diritti degli interessati, in particolare, per quanto riguarda il segreto professionale[115].

D'altro canto, l'obbligo del segreto professionale imposto ai titolari del trat- tamento e ai responsabili del trattamento con riferimento a determinati dati personali potrebbe limitare i diritti degli interessati, segnatamente il diritto a ricevere informazioni. Sebbene il regolamento generale sulla protezione dei dati contenga un elenco completo delle informazioni che, in linea di principio, devono essere fornite all'interessato nel caso in cui i dati personali non siano stati ottenuti dallo stesso, tale requisito di divulgazione non si applica qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri[116].

Il regolamento generale sulla protezione dei dati (RGPD) prevede la possibi- lità per gli Stati membri di stabilire per legge norme specifiche per tutelare il segreto professionale o altri obblighi di segretezza equivalenti e conciliare il diritto alla protezione dei dati personali e l'obbligo del segreto professionale[117].

Il RGPD stabilisce che gli Stati membri possono adottare norme specifiche sui poteri delle autorità di controllo rispetto ai titolari del trattamento o ai respon- sabili del trattamento soggetti all'obbligo del

segreto professionale. Tali norme specifiche si riferiscono al potere di ottenere accesso ai locali di un titolare del trattamento o di un responsabile del trattamento, ai suoi strumenti di tratta- mento dei dati e ai dati conservati, qualora tali dati personali siano stati ricevuti in seguito a un'attività protetta dall'obbligo di segretezza. Pertanto, le autorità di controllo incaricate della protezione dei dati devono rispettare gli obblighi di segreto professionale che vincolano i titolari del trattamento e i responsabili del trattamento. Inoltre, gli stessi membri delle autorità di controllo sono altresì tenuti al segreto professionale sia durante che dopo il loro mandato. Nell'ese- cuzione dei loro compiti, i membri e il personale delle autorità di controllo pos- sono venire a conoscenza di informazioni riservate. L'articolo 54, paragrafo 2, del regolamento prevede chiaramente il loro obbligo al segreto professionale con riferimento a tali informazioni riservate.

Il RGPD impone agli Stati membri di notificare alla Commissione le disposizioni adottate per conciliare la protezione dei dati e i principi sanciti dal regolamento con l’obbligo del segreto professionale.

1.3.3. Libertà di religione e di credo

La libertà di religione e di credo è tutelata dall’articolo 9 della CEDU (libertà di pensiero, di coscienza e di religione) e dall’articolo 10 della Carta dei diritti fondamentali dell’UE. I dati personali che rivelano convinzioni religiose o filoso- fiche sono considerati «dati sensibili» nell’ambito del diritto sia dell’UE sia del CdE, e il loro trattamento e utilizzo sono soggetti a una protezione rafforzata.

Esempio: il ricorrente nella causa *Sinak Isik c. Turchia*[118] era membro della comunità religiosa alevita, la cui confessione è influenzata dal sofismo e da altre credenze preislamiche, ed è considerata da alcuni pensatori una religione distinta e da altri una parte della religione islamica. Il ricorrente lamentava che, contro la sua volontà, la sua carta d’identità conteneva una casella che indicava la sua religione come «islamica» anziché «alevita». I giudici nazionali avevano respinto la sua richiesta di ottenere la dicitura
«alevita» sulla sua carta d’identità con la motivazione che tale termine designava un

sottogruppo dell’islam, e non una religione distinta. Egli si era quindi lamentato dinanzi alla Corte EDU del fatto che, senza il suo consenso, era stato obbligato a rivelare la sua fede in ragione dell’obbligo di indicare la religione di una persona sulla carta d’identità e che ciò costituiva una violazione del suo diritto alla libertà di religione e di coscienza, specialmente dal momento che la designazione «islam» sulla sua carta d’identità non rispecchiava la realtà.

La Corte EDU ha ribadito che la libertà di religione implica la libertà di manifestare la propria religione in modo collettivo, pubblicamente e nella cerchia di coloro che condividono la stessa confessione, ma anche individualmente e in privato. La legislazione nazionale applicabile all’epoca imponeva ai cittadini di portare una carta d’identità sulla quale compariva la loro religione, un documento che doveva essere presentato su richiesta di qualsiasi pubblica amministrazione o impresa privata. Tale obbligo non riconosceva il fatto che il diritto a manifestare la propria religione

comprendeva anche il caso inverso, vale a dire il diritto di non essere obbligati a rivelare le proprie convinzioni. Anche se il governo adduceva che la legislazione nazionale era stata modificata in modo da consentire alle persone di chiedere che la casella riservata alla religione fosse lasciata vuota, a parere della Corte il semplice fatto di dover domandare la cancellazione della religione poteva costituire divulgazione di un’informazione relativa al loro atteggiamento nei confronti della religione. Inoltre, quando le carte d’identità contengono uno spazio dedicato alla religione, il fatto di lasciarlo vuoto ha uno specifico significato, in quanto i titolari di una carta d’identità senza informazioni relative alla religione si distinguerebbero dalle persone che hanno una carta d’identità che indica le loro convinzioni religiose. La Corte EDU ha concluso che la normativa nazionale era in violazione dell’articolo 9 della CEDU.

La gestione di chiese e associazioni o comunità religiose può, tuttavia, richie- dere il trattamento dei dati personali dei loro membri, per rendere possibile la comunicazione e l’organizzazione delle attività nell’ambito della congrega- zione. Pertanto, le chiese e le associazioni religiose hanno spesso applicato norme in materia di trattamento dei dati personali. In base all’articolo 91 del regolamento generale sulla protezione dei dati, qualora si tratti di corpus com- pleti, possono continuare ad applicarsi purché siano resi conformi alle disposi- zioni del

regolamento. Le chiese e le associazioni religiose che prevedono tali norme devono essere soggette al controllo di un'autorità di controllo indipen- dente che può essere specifica, purché soddisfi le condizioni previste dal rego- lamento generale sulla protezione dei dati per tali autorità[119].

Le organizzazioni religiose possono effettuare il trattamento dei dati personali per diversi motivi, ad esempio, per rimanere in contatto con la loro congrega- zione o comunicare informazioni riguardanti eventi, manifestazioni religiose e feste di cui curano l'organizzazione, eventi di beneficenza, ecc. In alcuni Stati, le chiese devono tenere registri dei loro membri per motivi fiscali, dato che l'ap- partenenza a istituzioni religiose può avere un impatto sulle imposte pagate dai cittadini. In ogni caso, nell'ambito del diritto europeo, le convinzioni reli- giose sono dati sensibili e le chiese devono essere responsabili della gestione e del trattamento di tali dati, specialmente dal momento che le informazioni

trattate dalle organizzazioni religiose spesso riguardano bambini, anziani o altri membri vulnerabili della società.

1.3.4. Libertà delle arti e delle scienze

Un altro diritto da conciliare con i diritti al rispetto della vita privata e alla prote- zione dei dati è costituito dalla libertà delle arti e delle scienze, espressamente tutelato dall’articolo 13 della Carta dei diritti fondamentali dell’UE. Questo diritto è desunto in primo luogo dal diritto alla libertà di pensiero e di espressione e deve essere esercitato alla luce dell’articolo 1 della Carta (dignità umana). La Corte EDU considera la libertà delle arti e delle scienze tutelata dall’articolo 10 della CEDU[120]. Il diritto garantito dall’articolo 13 della Carta può anche essere soggetto alle limitazioni di cui all’articolo 52 , paragrafo 1, della Carta, che può essere interpretato anche alla luce dell’articolo 10, paragrafo 2, della CEDU[121].

Esempio: nella causa *Vereinigung bildender Künstler c. Austria*[122], i giudici austriaci hanno vietato all’associazione ricorrente di continuare a esporre un dipinto contenente le foto delle teste di alcune personalità pubbliche ritratte in atti sessuali. Un parlamentare austriaco, la cui foto era stata utilizzata nel dipinto, aveva intentato un’azione legale

contro l’associazione ricorrente per ottenere un’ingiunzione che vietasse l’esposizione del dipinto. Il giudice nazionale aveva emesso un’ingiunzione. La Corte EDU ha ribadito l’applicabilità dell’articolo 10 della CEDU alla comunicazione di idee che offendono, scioccano o preoccupano lo Stato o una fascia della popolazione. Coloro che creano, eseguono, distribuiscono o espongono opere d’arte contribuiscono allo scambio di idee e opinioni e lo Stato ha l’obbligo di non interferire indebitamente sulla loro libertà di espressione. Poiché il dipinto era un collage in cui erano utilizzate foto che ritraevano solo le teste dei soggetti, i cui corpi erano stati dipinti in modo irrealistico ed esagerato senza voler ovviamente riflettere o alludere alla realtà, la Corte EDU ha dichiarato altresì che «difficilmente il dipinto potrebbe essere interpretato come un’opera volta a rappresentare i dettagli della vita privata del soggetto raffigurato; esso, piuttosto, illustrerebbe la sua attività di politico», aggiungendo inoltre che «in tale veste, il soggetto raffigurato doveva mostrare una maggiore

tolleranza nei confronti della critica». Ponderando i diversi interessi in gioco, la Corte EDU ha rilevato che il divieto illimitato di un'ulteriore esposizione del dipinto era sproporzionato. La Corte ha concluso asserendo una violazione dell'articolo 10 della CEDU.

Il diritto europeo in materia di protezione dei dati riconosce altresì il grande valore della scienza per la società. Il regolamento generale sulla protezione dei dati e la Convenzione n. 108 modernizzata consentono la conservazione dei dati per periodi più lunghi, a condizione che i dati personali siano trattati unicamente a fini di ricerca scientifica o storica. Inoltre, e a prescindere dalle finalità iniziali di una specifica attività di trattamento, il successivo utilizzo dei dati personali per la ricerca scientifica non deve essere considerato un fine incompatibile[123]. Al contempo, devono essere adottate garanzie adeguate per tale trattamento, al fine di tutelare i diritti e le libertà degli interessati. Il diritto dell'UE o degli Stati membri può prevedere deroghe ai diritti dell'interessato come, ad esempio, ai diritti di accesso, rettifica, limitazione del trattamento e opposizione, se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici (cfr. anche le sezioni 6.1 e 9.4).

1.3.5. Protezione della proprietà intellettuale

Il diritto alla protezione della proprietà è sancito dall’articolo 1 del primo Pro- tocollo alla CEDU nonché dall’articolo 17, paragrafo 1, della Carta dei diritti fondamentali dell’UE. Un aspetto importante del diritto alla proprietà, partico- larmente rilevante per la tutela dei dati, è la protezione della proprietà intel- lettuale, esplicitamente menzionata nell’articolo 17, paragrafo 2, della Carta. Diverse direttive nell’ordinamento giuridico dell’UE sono volte all’effettiva tutela della proprietà intellettuale, in particolare, dei diritti d’autore. La pro- prietà intellettuale abbraccia non solo la proprietà letteraria e artistica, ma anche brevetti, marchi e diritti connessi.

Come chiarito dalla giurisprudenza della CGUE, la protezione del diritto fonda- mentale alla proprietà dev’essere conciliata con la protezione di altri diritti fon- damentali, in particolare con il diritto alla protezione dei dati[124]. Vi sono stati casi in cui istituzioni per la tutela dei diritti d’autore hanno chiesto ai fornitori

di accesso ad Internet di rivelare l’identità degli utenti di piattaforme di con- divisione di file in Internet. Tali piattaforme spesso consentono agli utenti di Internet di scaricare brani musicali gratuitamente, anche se questi sono protetti dal diritto d’autore.

Esempio: la causa *Promusicae c. Telefónica de España*[125] verteva sul rifiuto di un fornitore spagnolo di servizi di accesso a Internet (la società Telefónica) di rivelare a Promusicae, un’organizzazione senza fini di lucro di produttori musicali e editori di registrazioni musicali e audiovisive, i dati personali di talune persone alle quali quest’ultima forniva servizi di accesso a Internet. Promusicae ha chiesto la divulgazione delle informazioni in modo da poter av viare un procedimento civile nei confronti delle persone che, a suo avviso, utilizzavano un programma di scambio di file che forniva accesso ai fonogrammi i cui diritti di sfruttamento erano detenuti dai membri di Promusicae.

Il giudice spagnolo ha rinviato la questione alla CGUE, chiedendo se tali dati personali debbano essere comunicati, ai sensi del diritto dell’UE, nel contesto di un procedimento civile, per garantire l’effettiva tutela del diritto d’autore. Il giudice ha richiamato le direttive 2000/31, 2001/29 e 2004/48, anche alla luce degli articoli 17 e 47 della Carta. La CGUE ha

concluso che queste tre direttive, nonché la direttiva e-privacy (direttiva 2002/58), non ostano a che gli Stati membri stabiliscano l'obbligo di divulgare dati personali nel contesto di un procedimento civile, al fine di garantire la tutela effettiva del diritto d'autore.

La CGUE ha rilevato che il caso sollevava quindi la questione della necessaria conciliazione degli obblighi connessi alla tutela di diversi diritti fondamentali, ossia del diritto al rispetto della vita privata con i diritti alla tutela della proprietà e a un ricorso effettivo.

Essa ha concluso che «gli Stati membri sono tenuti, in occasione della trasposizione delle suddette direttive, a fondarsi su un'interpretazione di queste ultime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento di tali direttive, le autorità e i giudici

degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme alle dette direttive, ma anche provvedere a non fondarsi su un'interpretazione di esse che entri in conflitto con i summenzionati diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità»[126].

Esempio: la causa *Bonnier Audio AB e a. c. Perfect Communication Sweden AB*[127] riguardava l'equilibrio tra la tutela dei diritti di proprietà intellettuale e la tutela dei dati personali. Le ricorrenti, cinque case editrici titolari di diritti d'autore di 27 audiolibri, avevano intentato una causa dinanzi al giudice svedese adducendo la violazione di tali diritti d'autore a mezzo di un server FTP (un protocollo che consente la condivisione di file e il trasferimento di dati via Internet). Le ricorrenti avevano chiesto all'operatore Internet (ISP, Internet Service Provider) di ottenere la comunicazione del nome e del recapito della persona facente uso dell'indirizzo IP dal quale i file erano stati trasmessi. L'operatore Internet (ePhone) si era opposto a tale domanda, sostenendo che violava la direttiva 2006/24 (la direttiva sulla conservazione dei dati, invalidata nel 2014).

Il giudice svedese aveva rinviato la questione alla CGUE, chiedendo se la direttiva 2006/24 ostasse all'applicazione di una disposizione nazionale

fondata sull’articolo 8 della direttiva 2004/48 (direttiva sul rispetto dei diritti di proprietà intellettuale), che consente l’emissione di un’ingiunzione con la quale si chiede ad un operatore Internet di trasmettere a titolari di diritti d’autore informazioni riguardanti abbonati i cui indirizzi IP sono serviti a fini di violazioni. La domanda si basava sulla presunzione che il ricorrente avesse dimostrato la sussistenza di indizi effettivi dell’avvenuta violazione di un particolare diritto d’autore e che la misura risultava proporzionata.

La CGUE ha sottolineato che la direttiva 2006/24 riguardava esclusivamente il trattamento e la conservazione di dati generati dai fornitori di servizi di comunicazione elettronica a fini di indagine, di accertamento e perseguimento di reati gravi, nonché la loro trasmissione alle competenti autorità nazionali. Pertanto, una norma nazionale di recepimento della direttiva sul rispetto

dei diritti di proprietà intellettuale non rientra nel campo di applicazione della direttiva 2006/24 e non è, di conseguenza, preclusa dalla suddetta direttiva[128].

Per quanto riguarda la comunicazione del nome e del recapito in questione richiesta dalle ricorrenti, la CGUE ha stabilito che tale operazione costituisce trattamento di dati personali e rientra nella sfera di applicazione della direttiva 2002/58/CE (direttiva e-privacy). Essa ha inoltre rilevato che la comunicazione di tali dati era richiesta nell'ambito di un procedimento civile, a favore del titolare di un diritto d'autore, al fine di garantire la tutela effettiva del diritto d'autore e di conseguenza rientra, in considerazione del suo oggetto, nella sfera di applicazione della direttiva 2004/48[129].

La CGUE ha concluso che le direttive 2002/58 e 2004/48 devono essere interpretate nel senso che non ostano ad una normativa nazionale, come quella oggetto della causa principale, nella parte in cui tale normativa consente al giudice nazionale, dinanzi al quale sia stata proposta domanda di ingiunzione di comunicare dati di carattere personale, di ponderare, in funzione delle circostanze della specie e tenuto debitamente conto delle esigenze risultanti dal principio di proporzionalità, i contrapposti interessi in gioco.

1.3.6. Protezione dei dati e interessi economici

Nell’era digitale, o era dei megadati, i dati sono stati descritti come il «nuovo petrolio» dell’economia, per avere dato impulso all’innovazione e alla creatività[130]. Molte aziende hanno creato solidi modelli commerciali fondati sul trat- tamento dei dati e tale trattamento coinvolge spesso i dati personali. Alcune aziende sono convinte che norme specifiche relative alla protezione dei dati personali potrebbero, in pratica, comportare obblighi eccessivamente onerosi, con un conseguente impatto sui loro interessi economici. Viene così sollevata la questione se gli interessi economici dei responsabili del trattamento e dei

titolari del trattamento, o del pubblico generale, possano giustificare la restri- zione del diritto alla protezione dei dati.

Esempio: nella causa *Google Spain*[131], la CGUE ha stabilito che, in presenza di determinate condizioni, le persone hanno il diritto di chiedere ai motori di ricerca di eliminare i risultati dai loro indici di ricerca. Nel ragionamento svolto, la CGUE ha sottolineato il fatto che l'utilizzo di motori di ricerca e i risultati di ricerca elencati possono stabilire un profilo dettagliato di una persona. Queste informazioni possono riguardare un ampio aspetto della vita privata di una persona e, senza un motore di ricerca, non avrebbero potuto essere facilmente trovate o connesse tra loro. Ciò costituiva quindi un'ingerenza potenzialmente grave nei diritti fondamentali alla vita privata e alla protezione dei dati personali degli interessati.

La CGUE ha quindi esaminato se tale ingerenza possa essere giustificata. Per quanto riguarda l'interesse economico della società del motore di ricerca ad effettuare il trattamento, la CGUE ha dichiarato che «è giocoforza constatare che [l'ingerenza] non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati» e che «in linea di principio» i diritti fondamentali derivanti dagli articoli 7 e 8 della Carta prevalgono su tale interesse economico e

sull’interesse del pubblico a trovare tali informazioni in occasione di una ricerca concernente il nome dell’interessato[132].

Una delle considerazioni chiave del diritto europeo in materia di protezione dei dati è fornire alle persone un maggiore controllo sui loro dati personali. Soprattutto nell’era digitale, esiste uno squilibrio tra il potere delle entità commer- ciali che trattano e hanno accesso a grandi quantità di dati personali e il potere delle persone alle quali i dati personali appartengono di controllare le informa- zioni che le riguardano. La CGUE adotta un approccio caso per caso nel ponde- rare la protezione dei dati e gli interessi economici, come gli interessi dei terzi rispetto alle società per azioni e alle società a responsabilità limitata, come illu- strato nella sentenza *Manni*.

Esempio: la causa *Manni*[133] riguardava la pubblicazione dei dati personali di una persona in un registro pubblico delle imprese. Il sig. Manni aveva chiesto alla Camera di commercio di Lecce di cancellare i suoi dati personali da tale registro, avendo scoperto che i potenziali clienti, avvalendosi del registro avrebbero visto che egli era stato amministratore di una società dichiarata fallita più di un decennio prima. Queste informazioni pregiudicavano i suoi potenziali clienti e potevano avere un impatto negativo sui suoi interessi commerciali.

La CGUE è stata chiamata a stabilire se il diritto dell'UE riconosceva un diritto alla cancellazione nella fattispecie. Nel raggiungere le sue conclusioni, essa ha ponderato le norme dell'UE in materia di protezione dei dati e l'interesse commerciale del sig. Manni a ottenere la cancellazione delle informazioni riguardanti il fallimento della sua precedente società, con l'interesse del pubblico ad accedere alle informazioni. Essa ha riconosciuto che la pubblicità del registro delle imprese era prevista per legge e, segnatamente, da una direttiva dell'UE volta a facilitare l'accesso di terzi alle informazioni sulle società. La pubblicità era impor tante per tutelare gli interessi di terzi potenzialmente interessati a operare con una società specifica, dato che le società per azioni e le società a responsabilità limitata offrono come unica garanzia per i terzi il proprio patrimonio

sociale. Di conseguenza, «la pubblicità deve consentire ai terzi di conoscere gli atti essenziali della società, certe indicazioni che la concernono, in particolare le generalità delle persone che hanno il potere di obbligarla»[134].

Alla luce dell'importanza dello scopo legittimo perseguito dal registro, la CGUE ha stabilito che il sig. Manni non aveva il diritto di ottenere la cancellazione dei propri dati personali, dal momento che l'esigenza di tutelare gli interessi dei terzi nei confronti delle società per azioni e delle società a responsabilità limitata e di garantire la certezza del diritto, la lealtà delle transazioni commerciali e, pertanto, il buon funzionamento del mercato interno, prevalevano sui suoi diritti ai sensi della legislazione sulla protezione dei dati. Questo era particolarmente evidente in considerazione del fatto che le persone che scelgono di prendere parte agli scambi economici attraverso una società per azioni o una società a responsabilità limitata sono consapevoli

di essere tenute a rendere pubblici i dati relativi alle loro generalità e alle loro funzioni.

Pur ritenendo che nel caso di specie non vi fossero motivi per ottenere la cancellazione, la CGUE ha riconosciuto l'esistenza di un diritto di opposizione al trattamento, dichiarando che: «non si può [...] escludere che possano sussistere situazioni particolari in cui ragioni preminenti e legittime connesse al caso concreto della persona interessata giustifichino, in via eccezionale, che l'accesso ai dati personali ad essa relativi iscritti nel registro sia limitato, decorso un periodo di tempo suf ficientemente lungo [...] ai terzi che dimostrino un interesse specifico alla loro consultazione»[135].

La CGUE ha stabilito che spetta ai giudici nazionali valutare in ciascun caso, alla luce dell'insieme delle circostanze rilevanti dell'interessato, l'esistenza o l'assenza di ragioni legittime e preminenti che potrebbero, in via eccezionale, giustificare la limitazione all'accesso di terzi ai dati personali contenuti nei registri delle imprese. Nondimeno, essa ha precisato che, nel caso del sig. Manni, il solo presumere che la pubblicazione dei suoi dati personali nel registro influisse sulla sua clientela, non poteva essere sufficiente a costituire una simile ragione legittima e preminente. I potenziali clienti del sig. Manni avevano un interesse legittimo nelle informazioni concernenti il fallimento della sua precedente società.

L'ingerenza nei diritti fondamentali del sig. Manni e delle altre persone inserite nel registro al rispetto per la vita privata e alla protezione dei dati personali sanciti dagli articoli 7 e 8 della Carta rispondeva a una finalità di interesse generale ed era necessaria e proporzionata.

Pertanto, nella causa *Manni* la CGUE ha stabilito che i diritti alla protezione dei dati e della vita privata non prevalevano sugli interessi dei terzi ad accedere alle informazioni contenute nel registro delle imprese, rispetto alle società per azioni e alle società a responsabilità limitata.

2.1. Dati personali

- I dati personali sono tali se si riferiscono a una persona identificata o identifica- bile, l'«interessato».

- Per stabilire l'identificabilità di una persona, un titolare del trattamento, o un ter zo, deve considerare tut ti i mez zi di cui può ragionevolmente av valersi, come l 'individuazione, per identif icare det ta persona f isica diret tamente o indirettamente.

- Per autenticazione s’intende il processo teso a verificare se una persona possiede una certa identità e/o sia autorizzata a svolgere determinate attività.

- Esistono categorie particolari di dati, i cosiddetti dati sensibili, elencati nella Con- venzione n. 108 modernizzata e nel diritto dell’UE in materia di protezione dei dati, che richiedono una maggiore protezione e, pertanto, sono soggetti a un regime giuridico specifico.

- I dati sono anonimizzati quando non si riferiscono più a una persona identificata o identificabile.

- La pseudonimizzazione è una misura mediante la quale i dati personali non pos- sono essere attribuiti all’interessato senza informazioni aggiuntive, che sono conservate separatamente. La «chiave» che consente la re-identificazione degli interessati deve essere conservata separatamente e al sicuro. I dati sottoposti a un processo di pseudonimizzazione restano dati personali. Nel diritto dell’UE non esiste il concetto di «dati pseudonimizzati».

- I principi e le norme di protezione dei dati non si applicano alle informazioni ano- nimizzate. Essi si applicano, tuttavia, ai dati pseudonimizzati.

2.1.1. Aspetti principali del concetto di dati personali

Nel quadro del diritto dell'UE e del diritto del CdE, i «dati personali» sono defi- niti come qualsiasi informazione riguardante una persona fisica identificata o identificabile[136]. Si tratta di informazioni che riguardano una persona la cui identità è manifestamente chiara o può almeno essere accertata mediante l'ot- tenimento di informazioni supplementari. Per stabilire l'identificabilità di una persona, un titolare del trattamento, o un terzo, deve considerare tutti i mezzi di cui può ragionevolmente avvalersi, come l'individuazione, per identificare detta persona fisica direttamente o indirettamente, rendendo possibile trattare una persona diversamente da un'altra[137].

Con il trattamento di dati relativi a tale persona, quest'ultima viene definita «interessato».

L'interessato

Nel quadro del diritto dell'UE, le persone fisiche sono le uniche beneficiarie delle norme in materia di protezione dei dati[138] e solo gli esseri viventi sono tutelati dal diritto europeo in materia di protezione dei dati[139]. Il regolamento generale sulla protezione dei dati (RGPD) definisce dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Anche il diritto del CdE, in particolare la Convenzione n. 108 modernizzata, fa riferimento alla protezione delle persone fisiche per quanto riguarda il trattamento dei loro dati personali. Anche in questo caso, con l'espressione «dati a carattere personale», si intende ogni informazione concernente una persona fisica identificata o identificabile. Tale persona fisica o individuo, ai sensi rispet- tivamente del RGPD e della Convenzione n. 108 modernizzata, nel diritto in materia di protezione dei dati è denominata «interessato».

Anche le persone giuridiche godono di determinate tutele. Esiste una giuri- sprudenza della Corte EDU contenente alcune sentenze riguardanti ricorsi presentati da persone giuridiche e vertenti su violazioni del diritto alla protezione contro l'uso dei loro dati ai sensi dell'articolo 8 della CEDU. L'articolo 8 della CEDU riguarda sia il diritto al rispetto della vita privata e familiare sia il diritto al rispetto del

domicilio e della corrispondenza. La Corte può quindi esaminare questi casi nell'ambito di quest'ultimo, anziché nella sfera della vita privata.

Esempio: la causa *Bernh Larsen Holding AS e a. c. Norvegia*[140] riguardava una denuncia presentata da tre società norvegesi in merito a una decisione dell'autorità fiscale che ordinava loro di fornire agli ispettori fiscali una copia di tutti i dati contenuti nel server del computer condiviso dalle società.

La Corte EDU ha rilevato che un tale obbligo per le società ricorrenti costituiva un'ingerenza nel loro diritto al rispetto del «domicilio» e della «corrispondenza» ai sensi dell'articolo 8 della CEDU. Tuttavia, ha anche riscontrato che le autorità fiscali disponevano di garanzie efficaci e adeguate

contro ogni abuso: le società ricorrenti avevano ricevuto un largo preavviso, erano presenti e in grado di formulare osservazioni durante l'intervento in loco e il materiale doveva essere distrutto una volta che l'ispezione fiscale fosse stata portata a termine. In tali circostanze era stato conciliato, da un lato, il diritto delle società ricorrenti al rispetto del «domicilio» e della
«corrispondenza» e il loro interesse a proteggere la vita privata delle persone che lavorano per loro e, dall'altro lato, l'interesse pubblico a garantire un'ispezione efficiente ai fini dell'accertamento fiscale. La Corte EDU ha statuito che non vi era stata quindi alcuna violazione dell'articolo 8 della CEDU.

Ai sensi della Convenzione n. 108 modernizzata, la protezione dei dati inte- ressa, in primo luogo, la tutela delle persone fisiche; tuttavia, le parti contra- enti possono estendere, nel rispettivo diritto nazionale, la protezione dei dati alle persone giuridiche, quali società e associazioni. La relazione esplicativa alla Convenzione modernizzata precisa che il diritto nazionale può tutelare gli interessi legittimi delle persone giuridiche estendendo il campo di applicazione della Convenzione a tali soggetti[141]. La normativa dell'UE in materia di prote- zione dei dati non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare non riguarda le imprese dotate di personalità giuridica, compresi il nome e la forma della persona

giuridica e i suoi dati di contatto[142]. La direttiva e-privacy (direttiva relativa alla vita privata e alle comunicazioni elettroniche) tutela, tuttavia, la riservatezza delle comunicazioni e i legittimi interessi delle persone giuridiche con riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti[143]. Analogamente, il progetto di regolamento sull'ePrivacy estende la tutela alle persone giuridiche.

Esempio: nella causa *Volker und Markus Schecke e Hartmut Eifert c. Land Hessen*[144], la CGUE, riferendosi alla pubblicazione di dati personali relativi ai beneficiari di aiuti agricoli, ha considerato che «le persone giuridiche possono invocare la tutela degli artt. 7 e 8 della Carta nei confronti di una simile

identificazione solamente qualora la ragione sociale della persona giuridica identifichi una o più persone fisiche. [...I]l rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta, [è] riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile [...]»[145].

Nel contemperare l'interesse dell'UE a garantire la trasparenza nella concessione di aiuti da un lato, con i diritti fondamentali alla vita privata e alla protezione dei dati dei beneficiari di aiuti dall'altro, la CGUE ha considerato sproporzionata l'ingerenza in tali diritti fondamentali. Essa ha ritenuto che l'obiettivo della trasparenza avrebbe potuto essere raggiunto in modo efficace attraverso misure meno invasive per i diritti degli interessati. Tuttavia, nell'esaminare la proporzionalità della pubblicazione di informazioni relative alle persone giuridiche beneficiarie di aiuti, la CGUE ha raggiunto una conclusione diversa, affermando che tale pubblicazione non superava i limiti imposti dal principio di proporzionalità. Essa ha statuito che «la gravità della lesione del diritto alla protezione dei dati personali si presenta in maniera differente per le persone giuridiche e per le persone fisiche»[146]. Le persone giuridiche erano soggette ad obblighi più gravosi con riferimento alla pubblicazione dei dati che le riguardavano. La CGUE ha ritenuto che l'obbligo per le autorità nazionali di esaminare prima della pubblicazione, per ogni persona giuridica

beneficiaria, se i dati di quest'ultima identifichino persone fisiche associate graverebbe tali autorità di un onere amministrativo eccessivo. Pertanto, la normativa che imponeva una pubblicazione generalizzata di dati relativi alle persone giuridiche aveva rispettato un giusto equilibrio tra gli interessi coinvolti.

Natura dei dati

Qualsiasi informazione può essere ritenuta un dato personale, a condizione che si riferisca a una persona identificata o identificabile.

Esempio: la valutazione delle prestazioni lavorative di un dipendente effettuata da un supervisore e archiviata nel fascicolo personale del dipendente, costituisce un insieme di dati personali dello stesso dipendente.

Ciò è vero anche se potrebbe riflettere, in tutto o in parte, solo il parere personale del superiore come, per esempio, «il dipendente non si impegna nel lavoro», e non fatti concreti, come «il dipendente è stato assente per cinque settimane negli ultimi sei mesi».

I dati personali riguardano le informazioni sulla vita privata di una persona, com prese le at tività professionali, nonché le informazioni sulla sua vita pubblica.

Nella causa *Amann*,[147] secondo l'interpretazione della Corte EDU, l'espressione
«dati personali» non si limita alle questioni nella sfera privata di un individuo. Questo significato attribuito all'espressione «dati personali» è rilevante anche per il RGPD.

Esempio: nella causa *Volker und Markus Schecke e Hartmut Eifert c. Land Hessen*[148], la CGUE ha statuito che «[...] è irrilevante la circostanza che i dati pubblicati attengano ad attività professionali [...]. La Corte europea dei diritti dell'uomo ha dichiarato, a tale proposito, con riguardo all'interpretazione dell'art. 8 della Convenzione n. 108, che l'espressione "vita privata" non deve essere interpretata in modo restrittivo e che nessun motivo

di principio consente di escludere le attività professionali [...] dalla nozione di vita privata».

Esempio: nelle cause riunite *YS c. Minister voor Immigratie, Integratie en Asiel e Minister voor Immigratie, Integratie en Asiel c. M e S*[149], la CGUE ha stabilito che l'analisi giuridica contenuta in una bozza di decisione del servizio dell'immigrazione e delle naturalizzazioni riguardante richieste di titoli di soggiorno non costituisce di per sé dati personali, pur potendo comprendere dati personali.

La giurisprudenza della Corte EDU relativa all'articolo 8 della CEDU conferma la possibile difficoltà di operare una netta separazione tra le questioni della vita privata e quelle della vita professionale[150].

Esempio: nella causa *Bărbulescu c. Romania*[151], il ricorrente era stato licenziato per aver utilizzato il servizio Internet del suo datore di lavoro durante l'orario di lavoro, in violazione del regolamento interno. Il datore di lavoro aveva controllato le sue comunicazioni e le registrazioni, che mostravano messaggi di natura puramente privata, erano state prodotte dinanzi ai tribunali nazionali. Ritenendo applicabile l'articolo 8, la Corte EDU ha lasciato aperta la questione se le disposizioni restrittive del datore di lavoro lasciassero al richiedente un'aspettativa ragionevole in materia di vita privata, ma ritenuto, in ogni caso, che le istruzioni di un datore di lavoro non potevano ridurre a zero l'esercizio della vita privata sociale sul luogo di lavoro. Quanto agli argomenti sul merito, agli Stati contraenti doveva essere accordato un ampio margine di valutazione per stimare la necessità di adottare un quadro giuridico a disciplina delle condizioni in cui un datore di lavoro può regolamentare le comunicazioni non professionali, elettroniche o altro, dei propri dipendenti sul luogo di lavoro. Nondimeno, le autorità nazionali dovevano garantire che l'introduzione da parte del datore di lavoro di misure per controllare la corrispondenza e

altre comunicazioni, indipendentemente dalla portata e dalla durata di tali misure, fosse accompagnata da adeguate e sufficienti garanzie contro gli abusi. La proporzionalità e le garanzie procedurali contro l'arbitrarietà erano essenziali e la Corte EDU ha individuato una serie di fattori pertinenti nelle circostanze del caso. Tali fattori comprendevano, ad esempio, la portata del controllo dei dipendenti da parte del datore di lavoro e il grado di intrusione nella vita privata, le conseguenze per il dipendente e se fossero state fornite garanzie adeguate. Inoltre, le autorità nazionali dovevano garantire che il lavoratore, le cui comunicazioni erano state controllate, avesse accesso a un mezzo di ricorso dinanzi a un organo giurisdizionale competente a statuire, almeno in sostanza, sul rispetto dei criteri menzionati e sulla legittimità delle misure contestate. In questo caso, la Corte EDU ha rilevato una violazione dell'articolo 8, perché le autorità nazionali non avevano protetto in maniera adeguata il diritto del ricorrente al

rispetto della sua vita privata e della sua corrispondenza e, di conseguenza, non avevano trovato un equo equilibrio tra gli interessi in gioco.

Secondo il diritto sia dell'UE sia del CdE, le informazioni contengono dati riguardanti una persona se:

- un individuo è identificato o identificabile sulla base di tali informazioni, o
- un individuo, non identificato, può essere individuato attraverso tali informazioni in modo tale da consentire di svelare l'identità dell'interessato conducendo ulteriori ricerche.

Entrambi i tipi d'informazione sono tutelati in modo analogo dal diritto euro- peo in materia di protezione dei dati. L'identificabilità diretta o indiretta delle persone richiede una valutazione costante, «tenendo conto sia delle tecnolo- gie disponibili al momento del trattamento, sia degli sviluppi tecnologici»[152]. La Corte EDU ha ripetutamente dichiarato che la nozione di «dati personali» ai sensi della CEDU equivale a quella contenuta nella Convenzione n. 108, in particolare per quanto riguarda la condizione di persone identificate o identificabili[153].

Il RGPD stabilisce che si considera identificabile la persona fisica «che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»[154]. L'identificazione necessita quindi elementi che descrivano una per- sona in modo tale da renderla distinguibile da tutte le altre persone e ricono- scibile come individuo. Il nome di una persona è un esempio primario di tali elementi descrittivi e può identificare una persona direttamente. In alcuni casi, altri attributi possono avere un effetto analogo a un nome, rendendo una per- sona identificabile indirettamente. Un numero di telefono, il numero di previ- denza sociale e il numero di immatricolazione di un veicolo sono tutti esempi di informazioni che possono rendere identificabile una persona. È anche possibile utilizzare attributi, come file informatici, cookie e strumenti di sorveglianza del

traffico web, per identificare le persone individuando il loro comportamento e le loro abitudini. Come spiegato in un parere del Gruppo di lavoro articolo 29,
«[s]enza neanche cercare il nome e l’indirizzo di un soggetto è possibile cate- gorizzarlo sulla base di criteri socioeconomici, fisiologici, filosofici o di altro tipo, e attribuirgli alcune decisioni, tanto più che il punto di contatto (il com- puter) non richiede più necessariamente che ne sia svelata l’identità in senso stretto»[155]. La definizione di dati personali nell’ambito sia del CdE sia dell’UE, è suf ficientemente ampia da coprire tut te le possibilità di identificazione (e quindi tutti i livelli di identificabilità).

Esempio: nella causa *Promusicae c. Telefónica de España*[156], la CGUE ha statuito che «[n]on è contestata neppure la circostanza che la comunicazione, richiesta dalla Promusicae, dei nominativi e degli indirizzi di taluni utilizzatori di [una certa piattaforma per lo scambio di file su Internet] implica la messa a disposizione di dati personali, ossia informazioni concernenti persone fisiche identificate o identificabili, in conformità alla definizione di cui all’art. 2, lett. a), della direttiva 95/46 [attualmente articolo 4, paragrafo 1, del RGPD]. Tale comunicazione di informazioni che, secondo la Promusicae, vengono archiviate dalla Telefónica –

circostanza che quest'ultima non contesta – costituisce un trattamento di dati personali»[157].

Esempio: la causa *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] riguardava il rifiuto del prestatore di servizi Internet Scarlet di predisporre un sistema di filtraggio delle comunicazioni elettroniche realizzate tramite programmi per lo scambio di archivi, onde impedire gli scambi dei file che ledono i diritti d'autore protetti dalla SABAM, una società di gestione che rappresenta gli autori, i compositori e gli editori. La CGUE ha stabilito che gli indirizzi IP degli utenti «costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti».

Dal momento che molti nomi non sono univoci, per stabilire l'identità di una persona possono essere necessari ulteriori attributi, al fine di garantire che tale persona non venga confusa con altre. Talvolta può essere necessario combi- nare attributi diretti e indiretti per identificare la persona alla quale le informa- zioni si riferiscono. La data e il luogo di nascita sono mezzi utilizzati frequente- mente. In aggiunta, per distinguere meglio un cittadino da un altro, alcuni paesi hanno introdotto numeri personalizzati. Dati fiscali trasmessi[159], dati relativi a un richiedente un titolo di soggiorno contenuti in un documento amministra- tivo[160] e documenti riguardanti rapporti bancari e fiduciari[161] possono costitu- ire dati personali. I dati biometrici, come le impronte digitali, le foto digitali o le scansioni dell'iride, i dati relativi all'ubicazione e gli attributi online, acqui- siscono un'importanza sempre maggiore nell'identificazione delle persone nell'era tecnologica.

Ai fini dell'applicabilità del diritto europeo in materia di protezione dei dati, tuttavia, non è necessaria l'effettiva identificazione dell'interessato, ma è suf- ficiente che la persona sia identificabile. Una persona è considerata identifi- cabile se vi sono elementi sufficienti attraverso i quali la persona interessata può essere identificata, direttamente o indirettamente[162]. In base al conside- rando 26 del RGPD, il parametro di riferimento consiste nel determinare la pos- sibilità

che mezzi identificativi ragionevoli siano a disposizione e siano gestiti dai potenziali utenti delle informazioni, comprese le informazioni in possesso di destinatari terzi (cfr. la sezione 2.3.2).

Esempio: un'autorità locale, avendo deciso di raccogliere dati sulla velocità di percorrenza delle autovetture su strade locali, fotografa dette autovetture, registrando automaticamente l'ora e il luogo, al fine di trasmettere i dati all'autorità competente, cosicché quest'ultima possa elevare una contravvenzione a chi ha violato i limiti di velocità. Un interessato presenta un reclamo, sostenendo che il diritto in materia di protezione dei dati non prevede alcuna base giuridica che autorizzi l'autorità locale a raccogliere questo tipo di dati. L'autorità locale sostiene di non raccogliere dati personali in quanto, a suo avviso, le targhe sono anonime. L'autorità locale non avrebbe

alcuna autorità giuridica per accedere al registro d'immatricolazione generale e scoprire l'identità del proprietario dell'autovettura o del suo conducente.

Questo ragionamento non è conforme al considerando 26 del RGPD. Poiché la finalità della raccolta dei dati è chiaramente quella d'identificare e multare i conducenti in eccesso di velocità, è prevedibile che si tenterà di procedere all'identificazione. Anche se non dispongono di un mezzo identificativo diretto, le autorità locali trasmettono i dati all'autorità competente, ossia le forze di polizia, che dispongono di tali mezzi. Il considerando 26 delinea inoltre esplicitamente uno scenario in cui è prevedibile che ulteriori destinatari dei dati, diversi dall'utente che utilizza immediatamente i dati, possano tentare d'identificare la persona. Alla luce del considerando 26, l'azione dell'autorità locale equivale alla raccolta di dati su persone identificabili e, quindi, richiede una base giuridica ai sensi del diritto in materia di protezione dei dati.

Per «accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli svi- luppi tecnologici»[163].

Esempio: nella causa *Breyer c. Bundesrepublik Deutschland*[164], la CGUE ha considerato la nozione di identificabilità indiretta degli interessati. La controversia trattava di IP dinamici che cambiano a ogni nuova connessione a Internet. I siti Internet dei servizi federali tedeschi registravano e conservavano gli indirizzi IP dinamici al fine di contrastare attacchi informatici e avviare procedimenti penali ove necessario. Solo il fornitore di accesso a Internet utilizzato dal sig. Breyer conteneva le informazioni aggiuntive necessarie per identificarlo.

La CGUE ha ritenuto che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore ha reso accessibile al pubblico costituisce un dato personale qualora solamente un terzo, segnatamente il

fornitore di accesso, disponga delle informazioni necessarie a identificarla[165]. Essa ha affermato che «non si richiede che tutte le informazioni che consentono di identificare la persona interessata debbano essere in possesso di una sola persona» affinché un dato personale possa essere qualificato come dato personale.Gli utenti di un indirizzo IP dinamico registrato da un fornitore di servizi Internet possono essere identificati in determinate situazioni, ad esempio nell'ambito di un procedimento penale in caso di attacchi informatici, con l'aiuto di altri soggetti[166]. Secondo la CGUE, qualora il fornitore «disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone», ciò costituisce «un mezzo che può essere ragionevolmente utilizzato per identificare la persona interessata». Pertanto, tali dati sono considerati dati personali.

Nell'ambito del diritto del CdE, l'identificabilità è intesa in modo simile. La relazione esplicativa della Convenzione n. 108 modernizzata contiene una descrizione simile: la nozione di «identificabile» non fa riferimento solo all'i- dentità civile o giuridica della persona in quanto tale, ma anche a tutti gli ele- menti suscettibili di «individualizzare» o distinguere (e quindi trattare in modo diverso) una persona rispetto ad altre. Tale «individualizzazione»

potrebbe avere luogo, ad esempio, a partire da un numero di identificazione, uno pseu- donimo, dati biometrici o genetici, dati di localizzazione, un indirizzo IP o un altro identificatore, che rimandano a una persona specifica o a un dispositivo o insieme di dispositivi (computer, telefono portatile, macchina fotografica, con- solle di gioco, ecc.)[167]. Una persona non è considerata «identificabile» se la sua identificazione richiede tempi, sforzi o risorse irragionevoli. Tale è il caso, ad esempio, quando l'identificazione di un interessato richiederebbe operazioni eccessivamente complesse, lunghe e costose. L'irragionevolezza dei tempi, degli sforzi o delle risorse deve essere valutata caso per caso, tenendo conto di fattori quali la finalità del trattamento, i costi e benefici dell'identificazione, il tipo di titolare del trattamento e la tecnologia utilizzata[168].

Quanto alla forma in cui i dati personali sono archiviati o utilizzati, è importante osservare che essa non è rilevante ai fini dell'applicabilità del diritto in mate- ria di protezione dei dati. Le comunicazioni scritte o orali possono contenere dati personali e immagini[169], comprese le immagini da sistemi di televisione a circuito chiuso (CCTV)[170] o il suono[171]. Anche le informazioni registrate elet- tronicamente e le informazioni su supporto cartaceo possono costituire dati personali. Perfino campioni di cellule di tessuti umani, che registrano il DNA di una persona, possono costituire fonti da cui vengono estratti dati biometrici[172], a condizione che i dati si riferiscano alle caratteristiche genetiche ereditate o acquisite della persona, forniscano unicamente informazioni concernenti la loro salute o fisiologia e siano il risultato di un'analisi di un campione biologico pro- veniente da tale persona[173].

Anonimizzazione

Secondo il principio della limitazione della conservazione, contemplato dal RGPD, nonché dalla Convenzione n. 108 modernizzata (e discusso in maniera più approfondita nel capitolo 3), i dati devono essere conservati «in una forma che consenta l'identificazione degli interessati per un arco di tempo non supe- riore al conseguimento delle finalità per le quali sono trattati»[174]. Di conse- guenza, i dati devono essere cancellati o

anonimizzati qualora un titolare del trattamento voglia conservarli quando non ne ha più bisogno e non servono più al loro scopo iniziale.

Il processo di anonimizzazione dei dati significa che tutti gli elementi identifica- tivi sono eliminati da un insieme di dati personali, in modo da non consentire più

l'identificazione dell'interessato[175]. Nel suo parere 05/2014, il Gruppo articolo 29 per la tutela dei dati esamina l'efficacia e i limiti delle diverse tecniche di anoni- mizzazione[176]. Esso riconosce il valore potenziale di tali tecniche, ma sottolinea che talune tecniche non funzionano necessariamente in tutti i casi. Per trovare la soluzione ottimale in una situazione determinata, il processo di anonimizzazione appropriato dovrebbe essere deciso caso per caso. Indipendentemente dalla tec- nica utilizzata, l'identificazione deve essere preclusa in modo irreversibile. Que- sto significa che, affinché i dati siano anonimizzati, nessun mezzo identificativo può essere lasciato nelle informazioni che, con un ragionevole sforzo, potrebbe servire a identificare nuovamente la persona o le persone interessate[177]. Il rischio di re-identificazione può essere valutato tenendo conto «dei tempi, degli sforzi o delle risorse necessari in base alla natura dei dati, del contesto del loro utilizzo, delle tecniche di re-identificazione disponibili e dei relativi costi»[178].

Una volta resi completamente anonimi, i dati non sono più ritenuti personali e la legislazione in materia di protezione dei dati non è più applicabile.

Il RGPD stabilisce che la persona, o organizzazione, titolare del trattamento dei dati personali non può essere obbligata a conservare, acquisire o trattare ulte- riori informazioni per identificare l'interessato

al solo fine di rispettare il rego- lamento. Tuttavia, a questa regola è prevista una deroga significativa: qualora l'interessato, al fine di esercitare i diritti di accesso, rettifica, cancellazione, limitazione della trasformazione e della portabilità dei dati, fornisca al titolare del trattamento ulteriori informazioni che ne consentano l'identificazione, i dati precedentemente resi anonimi diventano nuovamente dati personali[179].

Pseudonimizzazione

Le informazioni personali contengono attributi come nome, data di nascita, sesso e indirizzo, o altri elementi che potrebbero portare all'identificazione. Il processo di pseudonimizzazione dei dati personali significa che tali attributi sono sostituiti da uno pseudonimo.

Il diritto dell’UE definisce la «pseudonimizzazione» come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attri- buiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati per- sonali non siano attribuiti a una persona fisica identificata o identificabile»[180]. Contrariamente ai dati anonimizzati, i dati pseudonimizzati rimangono dati per- sonali e sono quindi soggetti alla legislazione in materia di protezione dei dati. Anche se la pseudonimizzazione può ridurre i rischi per gli interessati sul piano della sicurezza, essa non si sottrae all’ambito di applicazione del RGPD.

Il RGPD riconosce diversi usi della pseudonimizzazione quale misura tecnica appropriata per migliorare la protezione dei dati ed è menzionata specificamente per la progettazione e la sicurezza del trattamento dei dati[181]. È inoltre una garanzia adeguata che potrebbe essere utilizzata per il trattamento dei dati per- sonali per finalità diverse da quelle per le quali sono stati inizialmente raccolti[182].

La pseudonimizzazione non è esplicitamente menzionata nella definizione giuridica della Convenzione n. 108 modernizzata del CdE Tuttavia, la relazione esplicativa della Convenzione

modernizzata n. 108 statuisce chiaramente che l'uso di uno pseudonimo o di qualsiasi identificatore/identità digitale non si tra- duce nell'anonimizzazione dei dati, dal momento che l'interessato può ancora essere identificabile o individualizzato[183]. Un modo per pseudonimizzare i dati è attraverso la crittografia degli stessi. Una volta che i dati sono stati pseudo- nimizzati, il collegamento a un'identità esiste sotto forma di pseudonimo asso- ciato alla chiave di decifratura. Senza tale chiave, identificare i dati pseudoni- mizzati è difficile. Tuttavia, chi ha diritto a utilizzare la chiave di decifratura è in grado di risalire facilmente all'identità. Occorre prestare particolare attenzione all'uso di chiavi crittografiche da parte di persone non autorizzate. Pertanto,
«[i] dati pseudonimizzati devono [...] essere considerati dati personali [...]»
disciplinati dalla Convenzione n. 108 modernizzata[184].

Autenticazione

Si tratta di una procedura con cui una persona può dimostrare di possedere una certa identità e/o è autorizzata a compiere determinate azioni, come accedere a una zona di sicurezza o prelevare denaro da un conto bancario. L'autenticazione può essere ottenuta confrontando i dati biometrici, come per esempio una foto o le impronte digitali nel passaporto, con i dati della persona che si presenta, per esempio, al controllo dell'immigrazione[185], o mediante la richiesta d'informazioni che dovrebbero essere note solo alla persona con una certa identità o autorizza- zione, per esempio un codice d'identificazione personale (PIN) o una password, o ancora richiedendo l'esibizione di un oggetto specifico, che dovrebbe essere in esclusivo possesso della persona con una certa identità o autorizzazione, come una tessera con microprocessore o una chiave per l'apertura di una cassetta di sicurezza bancaria. Oltre alla password e alle tessere con microprocessore, le firme elettroniche, talvolta insieme ai PIN, sono uno strumento particolarmente idoneo a identificare e autenticare una persona nelle comunicazioni elettroniche.

2.1.2. Categorie particolari di dati personali

Ai sensi del diritto dell'UE e del diritto del CdE, esistono categorie particolari di dati personali che,

per loro natura, possono presentare in fase di trattamento un rischio per gli interessati e pertanto devono godere di maggiore protezione. Tali dati sono soggetti a un principio del divieto e tale trattamento è lecito in presenza di un numero limitato di condizioni.

Nell'ambito della Convenzione n. 108 modernizzata (articolo 6) e del RGPD (articolo 9), le seguenti categorie sono considerate dati sensibili:

- dati personali che rivelano l'origine razziale o etnica;

- dati personali che rivelano le opinioni politiche, le convinzioni religiose o di altro tipo comprese le convinzioni filosofiche;

- dati personali che rivelano l'appartenenza sindacale;

- dati genetici e dati biometrici trattati al fine di identificare una persona fisica;

- dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Esempio: la causa *Bodil Lindqvist*[186] riguardava il riferimento, in una pagina Internet, a diverse persone, identificate con il loro nome o altri mezzi, ad esempio il loro numero di telefono o informazioni relative ai loro passatempi. La CGUE ha statuito che «l'indicazione che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisc[e] un dato personale relativo alla salute»[187].

Dati personali relativi a condanne penali e reati

La Convenzione n. 108 modernizzata comprende, nell'elenco delle catego- rie particolari di dati, i dati personali relativi a reati, procedimenti e condanne penali e le relative misure di sicurezza[188]. Nell'ambito del GDPR, i dati perso- nali relativi alle condanne penali e ai reati o a connesse misure di sicurezza non sono menzionati come tali nell'elenco delle categorie particolari di dati, ma sono trattati in un articolo separato. L'articolo 10 del RGPD stabilisce che il trattamento di tali dati può avvenire soltanto «sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli inte- ressati». Un registro completo contenente informazioni sulle condanne penali, d'altro canto, può essere tenuto soltanto sotto il controllo di autorità pubbliche specifiche[189]. Nell'UE, il

trattamento dei dati personali nel contesto dell'applica- zione della legge è disciplinato da uno strumento giuridico specifico, la direttiva 2016/680/UE[190]. La direttiva prevede norme specifiche di protezione dei dati, che sono vincolanti per le autorità competenti quando trattano dati personali specificamente a titolo di prevenzione, indagine, accertamento e persegui- mento di reati (cfr. la sezione 8.2.1).

2.2. Trattamento di dati personali

- «Trattamento di dati personali» si riferisce a qualsiasi operazione effettuata su dati personali.
- Il termine «trattamento» comprende il trattamento sia automatizzato che manuale.
- Ai sensi del diritto dell'UE, il «trattamento» si riferisce anche al trattamento manuale in archivi strutturati.
- Ai sensi del diritto del CdE, il diritto nazionale può estendere il significato di «trat- tamento» fino a includere il trattamento manuale.

2.2.1. Concetto di trattamento di dati personali

Il concetto di trattamento dei dati personali è inteso in maniera ampia nell'am- bito del diritto sia dell'UE sia del CdE: «[per] "trattamento di dati personali" [si intende] […] qualsiasi operazione […], come la raccolta, la registrazione, l'or- ganizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o

qualsiasi altra forma di messa a disposizione, il raffronto o l'inter- connessione, la limitazione, la cancellazione o la distruzione»[191], compiuta sui dati personali. La Convenzione n. 108 modernizzata aggiunge alla definizione la conservazione dei dati personali[192].

Esempio: nella causa *František Ryneš*[193], il sig. Ryneš aveva catturato, attraverso il sistema di sorveglianza domestico a circuito chiuso (CCTV) da lui installato per proteggere la sua proprietà, l'immagine di due individui che avevano mandato in frantumi alcune finestre della sua casa. La CGUE ha stabilito che la videosorveglianza comportante la registrazione e la conservazione di dati personali costituisce trattamento automatico di dati

personali e rientra nel campo di applicazione della normativa dell'UE in materia di protezione dei dati.

Esempio: nella causa *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*[194], il sig. Manni aveva chiesto la cancellazione dei propri dati personali dal registro di una società di rating, che lo collegavano al fallimento di una società immobiliare, con conseguente effetto negativo sulla sua reputazione. La CGUE ha stabilito che «nel trascrivere e conservare dette informazioni nel registro e nel comunicarle, se del caso, a terzi su richiesta, l'autorità incaricata della tenuta del registro effettua un "trattamento di dati personali", per il quale essa è "responsabile"».

Esempio: i datori di lavoro raccolgono e trattano i dati riguardanti i dipendenti, compresi i profili retributivi. Il fondamento giuridico che conferisce legalità a tali operazioni è il contratto di lavoro.

I datori di lavoro devono trasmettere i dati sulle retribuzioni del proprio personale alle autorità fiscali. Questa trasmissione di dati è considerata ug ualmente un «trattamento» ai sensi del term ine utilizzato nella Convenzione n. 108 modernizzata e nel RGPD. Tuttavia, in questo caso, il fondamento giuridico per tale divulgazione non sono i contratti di lavoro. È necessario che sussista una base giuridica supplementare per le operazioni di

trattamento che comportano il trasferimento dei dati sulle retribuzioni dal datore di lavoro alle autorità fiscali. Tale base giuridica è in genere costituita dalle disposizioni delle leggi fiscali nazionali. In assenza di tali disposizioni e di qualsiasi altro motivo legittimo per procedere al trattamento, questo trasferimento di dati personali sarebbe un trattamento illecito.

2.2.2. Trattamento automatizzato di dati personali

La protezione dei dati ai sensi della Convenzione n. 108 e del RGPD si applica pienamente al trattamento automatizzato di dati personali modernizzata.

Ai sensi del diritto dell'UE, il trattamento automatizzato di dati personali riguarda il «trattamento interamente o parzialmente automatizzato di dati personali»[195]. La Convenzione n. 108 modernizzata contiene una definizione simile[196]. In termini pratici, ciò significa che qualsiasi trattamento di dati per- sonali attraverso mezzi automatizzati con l'ausilio, ad esempio, di un personal computer, un dispositivo mobile o un router, è disciplinato dalle norme in mate- ria di protezione dei dati sia dell'UE sia del CdE.

Esempio: la causa *Bodil Lindqvist*[197] riguardava il riferimento, in una pagina Internet, a diverse persone, identificate con il loro nome o altri mezzi, ad esempio il loro numero di telefono o informazioni relative ai loro passatempi. La CGUE ha stabilito che «l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio con il loro numero telefonico, o fornendo informazioni riguardanti la loro situazione lavorativa e gli interessi da esse coltivati nel tempo libero, costituisc[e] un "trattamento di dati personali interamente o parzialmente automatizzato"»" ai sensi dell'art. 3, n. 1, della direttiva 95/46[198].

Esempio: nella causa *Google Spain SL, Google Inc c. Agencia Española de Protección de Datos (AEPD),*

Mario Costeja González[199], il sig. González aveva richiesto la cancellazione, o la modifica, di un link che collegava il suo nome nel motore di ricerca «Google search» a due pagine di un quotidiano che annunciava un'asta immobiliare per la riscossione coattiva di crediti previdenziali. La CGUE ha statuito che «esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca "raccoglie" dati siffatti, che egli "estrae", "registra" e "organizza" successivamente nell'ambito dei suoi programmi di indicizzazione, "conserva" nei suoi server e, eventualmente, "comunica" e "mette a disposizione" dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche»[200]. La CGUE ha concluso che tali

azioni costituiscono «trattamento», «senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali».

2.2.3. Trattamento non automatizzato di dati personali

Anche il trattamento manuale di dati richiede la protezione dei dati.

La protezione dei dati ai sensi del diritto dell'UE non è in alcun modo limitata al trattamento automatizzato di dati. Pertanto, conformemente al diritto dell'UE, la protezione dei dati si applica anche al trattamento di dati personali negli archivi manuali, ossia fascicoli cartacei appositamente strutturati[201]. Un archivio struttu- rato classifica un insieme di dati personali, rendendoli accessibili in base a deter- minati criteri. Ad esempio, se un datore di lavoro tiene un archivio cartaceo, in ordine alfabetico, dal titolo «congedi dipendenti», contenente tutti i dettagli dei congedi di cui il personale ha fruito nell'anno precedente, tale fascicolo costituirà un archivio manuale soggetto alle norme dell'UE in materia di protezione dei dati. La ragione alla base dell'estensione della protezione dei dati è la seguente:

- i fascicoli cartacei possono essere strutturati in modo tale che la ricerca d'informazioni sia resa semplice e rapida;

- la conservazione di dati personali in fascicoli cartacei strutturati favorisce l'elusione delle restrizioni previste dalla legge per il trattamento automatiz- zato di dati[202].

Ai sensi del diritto del CdE, la definizione di trattamento automatizzato ricono- sce che tra le varie operazioni automatizzate vi possano essere alcune fasi in cui è richiesto il trattamento manuale dei dati personali[203]. L'articolo 2, lettera c), della Convenzione n. 108 modernizzata stabilisce che «[q]uando non viene fatto ricorso ad un trattamento automatizzato, il trattamento dei dati costituisce un'o- perazione, o insiemi di operazioni, effettuate su dati personali nell'ambito di un insieme strutturato di tali dati, accessibili o disponibili in base a criteri specifici».

2.3. Utenti dei dati personali

- Chiunque determini i mezzi e le finalità del trattamento di dati personali altrui è un «titolare del trattamento» ai sensi del diritto in materia di protezione dei dati; se più persone prendono questa decisione congiuntamente, si parlerà di «conti- tolari del trattamento».

- Un «responsabile del trattamento» è una persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento.

- Un responsabile del trattamento diventa titolare del trattamento quando deter- mina egli stesso i mezzi e le finalità del trattamento dei dati.

- Qualsiasi persona alla quale vengano c omunicati dati personali è un «destinatario».

- Per «terzo» s'intende una persona fisica o giuridica che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autoriz- zate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

- Il consenso come base giuridica per il trattamento dei dati personali deve essere una manifestazione di volontà libera, informata, specifica e inequivocabile con la quale viene manifestato l'assenso, mediante azione positiva, che i dati personali siano oggetto di trattamento.

- Il trattamento di categorie particolari di dati sensibili sulla base del consenso richiede il consenso esplicito.

2.3.1. Titolari del trattamento e responsabili del trattamento

La funzione di titolare del trattamento o responsabile del trattamento implica quale principale conseguenza la responsabilità giuridica dell'ottemperanza ai rispettivi obblighi previsti dal diritto in materia di protezione dei dati. Nel set- tore privato questa responsabilità grava di solito su una persona fisica o giu- ridica, mentre nel settore pubblico spetta generalmente a un'autorità. Esiste una distinzione significativa tra un titolare del trattamento e un responsabile del trattamento: il primo è la persona fisica o giuridica che determina le fina- lità e i mezzi del trattamento, mentre il secondo è la persona fisica o giuridica

che tratta i dati per conto del titolare del trattamento, seguendo istruzioni precise. In linea di principio, il titolare del trattamento esercita il controllo sul trattamento e su chi ne ha la responsabilità, compresa la responsabilità legale. Tuttavia, con la riforma delle norme sulla protezione dei dati, i responsabili del trattamento hanno ora l'obbligo di conformarsi a molti dei requisiti appli- cabili ai titolari del trattamento. Ad esempio, ai sensi del RGPD, i responsabili del trattamento tengono un registro di tutte le categorie di attività relative al trattamento, per dimostrare il rispetto degli obblighi di cui al regolamento[204]. I responsabili del trattamento devono, inoltre, mettere in atto misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento[205], designare un responsabile della protezione dei dati in determinate situazioni[206] e infor- mare il titolare del trattamento di eventuali violazioni[207].

Se una persona abbia la capacità di decidere e determinare la finalità i e mezzi del trattamento, dipenderà dagli elementi fattuali o dalle circostanze del caso. Secondo la definizione di titolare del trattamento di cui al RGPD, possono essere titolari del trattamento persone fisiche, persone giuridiche o qualsiasi altro organismo. Tuttavia, il Gruppo di lavoro articolo 29 ha sottoli- neato che, per fornire agli individui un'entità più stabile per l'esercizio dei loro diritti, «sarebbe

preferibile considerare come responsabile del trattamento la società o l'organismo in quanto tali piuttosto che una specifica persona al loro interno»[208]. Ad esempio, un'azienda che vende forniture sanitarie a pro- fessionisti è titolare del trattamento per quanto riguarda la compilazione e la gestione della lista di distribuzione di tutti i professionisti in una data area; non lo è il responsabile delle vendite, che utilizza e gestisce di fatto l'elenco.

Esempio: quando la divisione marketing operante in seno alla società Sunshine prevede di trattare i dati per uno studio di mercato, il titolare del trattamento sarà la società Sunshine e non i dipendenti della divisione in questione. La divisione marketing non può essere il titolare del trattamento, essendo priva di personalità giuridica distinta.

Le persone fisiche possono essere titolari del trattamento ai sensi del diritto sia dell’UE sia del CdE. Tuttavia, i privati, nel trattare i dati relativi ad altri nell’am- bito di attività a carattere esclusivamente personale o domestico, non rien- trano nell’ambito di applicazione delle norme del RGPD e della Convenzione n. 108 modernizzata, e non sono considerati titolari del trattamento[209]. Un indi- viduo che mantiene la propria corrispondenza, un diario personale che descrive eventi con amici e colleghi e i dati sanitari di membri della famiglia, può essere esonerato dalle norme sulla protezione dei dati, dal momento che tali attività potrebbero essere a carattere esclusivamente personale o meramente dome- stico. Il RGPD precisa inoltre che le attività a carattere personale o domestico potrebbero comprendere anche l’uso dei social network e attività online intra- prese nel quadro di tali attività[210]. Al contrario, le norme in materia di prote- zione dei dati si applicano in toto ai titolari del trattamento e ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell’ambito di attività a carattere personale o domestico (ad esempio, le piattaforme di social networking).[211]

L’accesso dei cittadini a Internet e la possibilità di utilizzare piattaforme per il commercio elettronico, social network e siti di blogging per condividere infor- mazioni personali riguardanti se stessi e altre persone, rendono sempre più difficile separare il

trattamento di dati personali da quello di dati non perso- nali[212]. Se le attività abbiano carattere esclusivamente personale o domestico dipende dalle circostanze.[213] Le attività che presentano aspetti professionali o commerciali non possono rientrare nell'esenzione per l'esercizio di attività a carattere personale o domestico[214]. Pertanto, se l'entità e la frequenza del trattamento dei dati suggerisce un'attività professionale o a tempo pieno, un privato potrebbe essere considerato titolare del trattamento. Oltre al carattere

professionale o commerciale dell'attività di trattamento, un altro fattore che deve essere preso in considerazione è se i dati personali siano messi a dispo- sizione di un vasto numero di persone, ovviamente esterne alla sfera privata dell'individuo. La giurisprudenza relativa alla direttiva sulla tutela dei dati ha rilevato che il diritto in materia di protezione dei dati trova applicazione quando un soggetto privato, utilizzando Internet, pubblica dati relativi ad altri in un sito Internet pubblico. La CGUE non ha ancora statuito su fatti simili nel quadro del RGPD, il quale fornisce maggiori orientamenti sugli argomenti che potrebbero esulare dall'ambito di applicazione della legislazione in materia di protezione dei dati in base all'«eccezione relativa alle attività a carattere domestico», come l'uso dei social media per scopi personali.

Esempio: la causa *Bodil Lindqvist*[215] riguardava il riferimento, in una pagina Internet, a diverse persone, identificate con il loro nome o altri mezzi, ad esempio il loro numero di telefono o informazioni relative ai loro passatempi. La CGUE ha sostenuto che «l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi [...], costituisce un "trattamento di dati personali interamente o parzialmente automatizzato" ai sensi dell'art. 3, n. 1, della direttiva 95/46»[216].

Tale trattamento di dati personali non rientra fra le attività a carattere strettamente personale o domestico, che esulano dall’ambito di applicazione della direttiva sulla tutela dei dati, dal momento che tale eccezione «deve [...] interpretarsi nel senso che comprende unicamente le attività che rientrano nell’ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone»[217].

Secondo la CGUE, in determinate circostanze, anche le registrazioni video di una telecamera di sicurezza installata da un privato possono rientrare nell'ambito nella legislazione dell'UE in materia di protezione dei dati.

Esempio: nella causa *František Ryneš*[218], il sig. Ryneš aveva catturato, attraverso il sistema di sorveglianza domestico a circuito chiuso (CCTV) da lui installato per proteggere la sua proprietà, l'immagine di due individui che avevano mandato in frantumi alcune finestre della sua casa. La registrazione era stata quindi consegnata alla polizia e fatta valere nel corso del procedimento penale.

La CGUE ha stabilito che «[p]osto che una videosorveglianza [...] si estende, anche se solo parzialmente, allo spazio pubblico, e pertanto è diretta verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, essa non può essere considerata un'attività esclusivamente "personale o domestica" [...]»[219].

Titolare del trattamento

Nell'ambito del diritto dell'UE, un titolare del trattamento viene definito come qualcuno che «singolarmente o insieme ad altri, determina le

finalità e i mezzi del trattamento di dati personali[220]». Il titolare del trattamento stabilisce il motivo e la modalità del trattamento.

Nell’ambito del diritto del CdE, la Convenzione n. 108 modernizzata definisce
«titolare del trattamento» «la persona fisica o giuridica, l’autorità pubblica, il servizio, l’agenzia od ogni altro organismo che, da solo o insieme ad altri, eser- cita il potere decisionale sul trattamento dei dati[221]». Tale potere decisionale riguarda le finalità e i mezzi del trattamento, nonché le categorie di dati da trattare e l’accesso ai dati[222]. Se tale potere sia conferito per designazione giu-

ridica o derivi da circostanze fattuali, è una questione che deve essere decisa caso per caso[223].

Esempio: la causa *Google Spain*[224] era stata intentata da un cittadino spagnolo che chiedeva la soppressione da Google di un vecchio articolo di giornale concernente antefatti finanziari che lo riguardavano.

Alla CGUE è stato chiesto se Google, in qualità di gestore di un motore di ricerca, fosse il «titolare» del trattamento ai sensi dell'articolo 2, lettera d), della direttiva sulla tutela dei dati[225]. La CGUE ha considerato un'ampia definizione della nozione di «responsabile», per garantire una «tutela efficace e completa delle persone interessate»[226].La CGUE ha stabilito che il gestore del motore di ricerca determinava le finalità e i mezzi dell'attività e rendeva i dati, fatti apparire su una pagina Internet da editori di siti web, accessibili a qualsiasi utente di Internet che effettuasse una ricerca a partire dal nome della persona interessata[227]. Di conseguenza, la CGUE ha stabilito che Google può essere considerato come «responsabile» del trattamento[228].

Quando un titolare del trattamento, o un responsabile del trattamento, non è sta- bilito nell'UE, tale società

deve designare per iscritto un rappresentante nell'Unione[229]. Il RGPD sottolinea che il rappresentante deve essere stabilito «in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato»[230]. Se nessun rappresentante è designato, un'azione legale può ancora essere avviata contro il titolare del trattamento o il responsabile del trattamento[231].

Contitolarità

Il RGPD stabilisce che allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Ciò significa che decidono insieme di trattare i dati per una finalità comune[232]. La Convenzione n. 108 modernizzata prevede anche la possibilità di più titolari o contitolari del trattamento nel quadro del CdE[233].

Il Gruppo di lavoro articolo 29 osserva che la contitolarità può assumere varie forme e la partecipazione dei diversi titolari del trattamento alle attività di controllo può differire[234]. Tale flessibilità permette di tenere conto della crescente complessità della realtà attuale del trattamento dei dati[235]. I contitolari del trattamento devono quindi determinare in un accordo specifico le rispettive responsabilità per il rispetto degli obblighi previsti dal regolamento[236].

La contitolarità determina la responsabilità comune per un'attività di trattamento[237]. Nell'ambito del diritto dell'UE, questo significa che ogni titolare del trattamento o responsabile del trattamento può essere considerato responsabile in solido per l'intero ammontare del danno causato dal trattamento effettuato in maniera congiunta, al fine di garantire il risarcimento effettivo dell'interessato[238].

Esempio: una banca dati riguardante i clienti insolventi, gestita congiuntamente da diversi istituti di credito, è un esempio tipico di contitolarità. Quando un soggetto presenta una richiesta relativa all’apertura di una linea di credito presso una banca che condivide la titolarità del trattamento, le banche controllano le informazioni presenti nella banca dati per decidere consapevolmente sul merito creditizio del richiedente.

Le disposizioni di legge non indicano espressamente se la contitolarità neces- siti che la finalità comune sia la stessa per ognuno dei titolari del trattamento

o se sia sufficiente la parziale corrispondenza delle rispettive finalità. Attual- mente, a livello europeo non vi è ancora giurisprudenza in materia. Nel suo parere del 2010 sui titolari e sui responsabili del trattamento, il Gruppo di lavoro ar ticolo 29 af ferma che i contitolari del trat tamento possono con- dividere tutte le finalità e tutti gli strumenti di un trattamento, alcune fina- lità o mezzi, o una parte di essi[239]. Mentre nel primo caso la relazione tra i diversi attori sarebbe molto stretta, nel secondo caso la relazione sarebbe più distante.

Gruppo di lavoro articolo 29 propende per un'interpretazione più ampia del con- cetto di contitolarità allo scopo di permettere una certa flessibilità che tenga conto della crescente complessità degli odierni trattamenti dei dati[240]. Una causa concernente la Society for Worldwide Interbank Financial Telecommunica- tion (SWIFT) illustra la posizione del Gruppo di lavoro articolo 29.

Esempio: nella cosiddetta causa SWIFT, gli istituti bancari europei ricorrevano alla SWIFT, inizialmente quale responsabile del trattamento, per operazioni inerenti al trasferimento di dati nel corso di operazioni bancarie. La SWIFT comunicava tali dati sulle operazioni bancarie, conservati in un centro di assistenza informatica negli Stati Uniti (USA), al dipartimento del Tesoro, senza ricevere istruzioni esplicite in tal senso da parte degli istituti bancari

europei che usufruivano dei suoi servizi. Il Gruppo di lavoro articolo 29, nel valutare la legittimità di questa situazione, giungeva alla conclusione che gli istituti bancari europei che si avvalevano dei servizi della SWIFT, così come la SWIFT stessa, dovevano essere considerati contitolari responsabili nei confronti dei clienti europei per la divulgazione dei loro dati alle autorità statunitensi[241].

Responsabile del trattamento

Ai sensi del diritto dell'UE si definisce responsabile del trattamento il soggetto che tratta dati personali per conto del titolare del trattamento[242]. Le attività

affidate a un responsabile del trattamento possono essere limitate a un com- pito o a un contesto molto specifico o possono essere molto generali, abbracciando molti aspetti.

Ai sensi del diritto del CdE, il significato di responsabile del trattamento è lo stesso di quello previsto dal diritto dell'UE[243].

Oltre a elaborare i dati altrui, i responsabili del trattamento saranno anche tito- lari del trattamento in quanto tali quando eseguono il trattamento per proprio conto, come per esempio la gestione dei propri dipendenti, l'amministrazione delle vendite e la tenuta della contabilità.

Esempio: la società Everready è specializzata nel trattamento di dati per la gestione delle risorse umane per altre aziende. In questa funzione, Everready è responsabile del trattamento. Tuttavia, quando tratta i dati dei propri dipendenti, Everready è il titolare delle operazioni di trattamento dei dati, che svolge per adempiere i propri obblighi di datore di lavoro.

Rapporto tra titolare del trattamento e responsabile del trattamento

Come visto in precedenza, il titolare del trattamento è definito come colui che determina le finalità e i mezzi del trattamento. Il RGPD stabilisce chiaramente che il responsabile del trattamento non può trattare dati personali se non è istru- ito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'U- nione o degli Stati membri[244]. Il contratto tra il titolare e il responsabile del tratta- mento è un elemento essenziale della loro relazione ed è un obbligo giuridico[245].

Esempio: il direttore della società Sunshine decide che la società Cloudy, specializzata nell'archiviazione di dati nel «cloud», venga incaricata di gestire i dati dei clienti della Sunshine. La società Sunshine rimane il titolare del trattamento e la società Cloudy è solo un responsabile del trattamento in

quanto, in base al contratto, Cloudy può utilizzare i dati dei clienti della società
Sunshine solo per le finalità definite da quest'ultima.

Se il potere di determinare i mezzi del trattamento è delegato a un responsa- bile, il titolare del trattamento deve comunque poter esercitare un adeguato controllo sulle decisioni del responsabile in merito ai mezzi del trattamento. La responsabilità generale spetta ancora al titolare del trattamento, che deve sorvegliare i responsabili del trattamento onde garantire che le loro decisioni siano conformi al diritto in materia di protezione dei dati e alle sue istruzioni.

Inoltre, se un responsabile del trattamento non rispetta le condizioni per il trat- tamento dei dati come prescritto dal titolare del trattamento, detto responsa- bile del trattamento diventa titolare del trattamento, almeno nella misura in cui non si è attenuto alle istruzioni del titolare del trattamento. Molto proba- bilmente tale situazione converte il responsabile del trattamento in un titolare del trattamento che agisce in maniera illecita. A sua volta, il titolare del trat- tamento originario dovrà spiegare come sia stato possibile che il responsabile del trattamento sia venuto meno al suo mandato[246]. Infatti, il Gruppo di lavoro articolo 29 tende a presupporre che in questi casi si realizzi una situazione di contitolarità, poiché quest'ultima

tutela in modo ottimale gli interessi degli interessati[247].

Possono sussistere anche problemi circa la ripartizione della responsabilità qua- lora il titolare del trattamento sia una piccola impresa e il responsabile una grande azienda in grado di dettare le condizioni dei propri servizi. In tali circostanze, tut- tavia, il Gruppo di lavoro articolo 29 afferma che in casi del genere il livello di responsabilità non dovrebbe ridursi sulla base della sperequazione economica, e che occorre attenersi all'interpretazione del concetto di titolare del trattamento[248].

Per motivi di chiarezza e trasparenza, i dettagli del rapporto tra un titolare del trattamento e un responsabile del trattamento devono essere disciplinati da un

contratto scritto[249]. Il contratto deve includere, in particolare, la materia disci- plinata, la natura, la finalità e la durata del trattamento, il tipo di dati personali e le categorie di interessati. Esso dovrebbe prevedere anche gli obblighi e i diritti del responsabile del trattamento, quali i requisiti in materia di riserva- tezza e sicurezza. La mancata stipula di tale contratto costituisce una viola- zione dell'obbligo del titolare del trattamento di fornire una documentazione scritta delle responsabilità reciproche e potrebbe dar luogo a sanzioni. Quando il danno è cagionato per avere agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento, la responsabilità non è solo di quest'ultimo, ma anche del responsabile del trattamento[250]. Il responsabile del trattamento deve tenere un registro di tutte le categorie di attività rela- tive al trattamento svolte per conto del titolare del trattamento[251]. Su richie- sta, tale registro deve essere messo a disposizione dell'autorità di controllo, dal momento che il titolare del trattamento e il responsabile del trattamento devono entrambi cooperare con tale autorità nell'esecuzione dei suoi com- piti[252]. I titolari e i responsabili del trattamento hanno altresì la possibilità di aderire ad un codice di condotta approvato o a un meccanismo di certificazione per dimostrare la loro conformità ai requisiti del RGPD[253].

I responsabili del trattamento potrebbero voler delegare alcuni compiti ad altri responsabili di secondo livello. Ciò è giuridicamente possibile, a condizione che siano stipulate clausole contrattuali appropriate tra il titolare del tratta- mento e il responsabile del trattamento, anche rispetto all'eventuale neces- sità dell'autorizzazione del titolare in ogni singolo caso ovvero di una semplice informativa data a quest'ultimo. Il RGPD stabilisce che il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità qua- lora il responsabile di secondo livello ometta di adempiere ai propri obblighi in materia di protezione dei dati[254].

Ai sensi del diritto del CdE, è pienamente applicabile l'interpretazione dei concetti di titolare del trattamento e responsabile del trattamento illustrati in precedenza[255].

2.3.2. Destinatari e terzi

La differenza tra queste due categorie di persone o entità introdotte dalla direttiva sulla tutela dei dati risiede principalmente nel loro rapporto con il titolare del trattamento e, di conseguenza, nel tipo di autorizzazione a questi conferita ai fini dell'accesso ai dati personali in possesso di detto titolare del trattamento.

Un «terzo» è un soggetto diverso dal titolare del trattamento e dal responsa- bile del trattamento. Ai sensi dell'articolo 4, paragrafo 10, del RGPD, si intende per terzo «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile». Questo significa che le per- sone che lavorano in un'impresa giuridicamente distinta dal titolare del trat- tamento, anche se facente parte di uno stesso gruppo o holding, saranno (o faranno parte di) «terzi». Per contro, le succursali di una banca che trattano dati contabili della clientela sotto l'autorità diretta della sede centrale non dovrebbero essere considerate come «terzi»[256].

Il termine «destinatario» è più ampio rispetto a quello di «terzi». Ai sensi dell'articolo 4, paragrafo 9, del RGPD, un destinatario è «la persona fisica o

giu- ridica, l’autorità pubblica, il servizio o un altro organismo che riceve comunica- zione di dati personali, che si tratti o meno di terzi». Il destinatario può essere una persona esterna al titolare o al responsabile del trattamento – in tal caso sarebbe un terzo – o qualcuno interno al titolare o al responsabile del tratta- mento, come per esempio un dipendente o un altro reparto all’interno della stessa azienda o autorità.

La distinzione tra destinatari e terzi è importante solo in ragione delle condi- zioni previste per la legittima divulgazione dei dati. I dipendenti di un titolare o di un responsabile del trattamento possono essere destinatari dei dati perso- nali, senza ulteriore obbligo giuridico, se prendono parte alle operazioni di trat- tamento del titolare o del responsabile del trattamento. Per contro, un terzo, essendo distinto dal titolare o dal responsabile del trattamento, non è autoriz- zato a utilizzare i dati personali trattati dal titolare del trattamento, salvo speci- fiche motivazioni giuridiche nel contesto di un caso particolare.

Esempio: il dipendente di un titolare del trattamento, che utilizza i dati personali nell'ambito dei compiti affidatigli dal datore di lavoro, è un destinatario dei dati, ma non un terzo, dal momento che utilizza i dati in nome e dietro istruzioni di detto titolare del trattamento. Ad esempio, se un datore di lavoro comunica dati personali riguardanti i propri dipendenti al dipartimento delle risorse umane, in considerazione delle prossime valutazioni delle prestazioni, il team delle risorse umane sarà destinatario dei dati personali, dal momento che questi ultimi gli sono stati comunicati nel corso del trattamento per il titolare dello stesso.

Se, tuttavia, l'organizzazione fornisce dati relativi ai propri dipendenti a una società di formazione che li utilizzerà per personalizzare un programma di formazione per i dipendenti, la società di formazione è un terzo. Il motivo è che la società di formazione non gode di legittimità o autorizzazione specifica (che nel caso delle «risorse umane» deriva dal rapporto di lavoro con il titolare del trattamento) per trattare tali dati personali. In altre parole, non hanno ricevuto le informazioni nell'ambito del loro lavoro con il titolare del trattamento.

2.4. Consenso

- Il consenso come base giuridica per il trattamento dei dati personali deve essere volontario, consapevole, specifico e inequivocabile, e l’assenso a che i dati per- sonali siano oggetto di trattamento deve essere manifestato mediante azione positiva.

- Il trattamento di categorie particolari di dati richiede il consenso esplicito.

Come sarà esaminato in dettaglio nel capitolo 4, il consenso è uno dei sei motivi legittimi per il trattamento dei dati personali. Per consenso s’intende
«qualsiasi manifestazione di volontà libera, specifica, informata e inequivoca- bile dell’interessato»[257].

Il diritto dell'UE prevede diversi elementi per la validità del consenso, volti a garantire che gli interessati intendano realmente acconsentire a uno specifico uso dei loro dati[258]:

- Il consenso deve essere espresso mediante un atto positivo chiaro con il quale l'interessato manifesta l'intenzione libera, specifica, consapevole e inequivocabile di accettare il trattamento dei propri dati personali. Tale atto può essere un'azione o una dichiarazione.

- L'interessato deve avere il diritto di revocare il consenso in qualsiasi momento.

- Nel contesto di una dichiarazione scritta che riguarda anche altre questioni, come i «termini di servizio», la richiesta di consenso deve essere espressa utilizzando un linguaggio semplice e chiaro e in forma comprensibile e facil- mente accessibile, in modo che distingua chiaramente il consenso dalle altre questioni; se costituisce una violazione del RGPD, una parte di tale dichiarazione non sarà vincolante.

Il consenso sarà valido nell'ambito del diritto in materia di protezione dei dati solo se tutti questi requisiti sono soddisfatti. Il titolare del trattamento ha la responsabilità di dimostrare che l 'interessato ha prestato il proprio consenso al trattamento dei propri dati personali[259]. Gli

elementi necessari ai fini della validità del consenso verranno esaminati ulteriormente nella sezione 4.1.1. concernente i legittimi presupposti per il trattamento dei dati personali.

La Convenzione n. 108 non contiene una definizione di consenso, che è lasciata alla competenza del diritto nazionale. Tuttavia, ai sensi del diritto del CdE, gli elementi necessari perché il consenso sia valido corrispondono a quelli illustrati in precedenza[260].

Ulteriori requisiti previsti dal diritto civile per un valido consenso, come la capa- cità giuridica, si applicano ovviamente anche nel contesto della protezione dei

dati, in quanto tali requisiti sono presupposti giuridici fondamentali. Il consenso non valido, in quanto accordato da persone prive di capacità giuridica, si tra- durrà nell'assenza di una base giuridica per il trattamento dei dati di tali per- sone. Per quanto riguarda la capacità giuridica dei minori di stipulare contratti, il RGPD stabilisce che le sue disposizioni concernenti l'età minima per ottenere un consenso valido non pregiudicano le disposizioni generali del diritto dei con- tratti degli Stati membri[261].

Il consenso deve essere espresso in maniera chiara, in modo da non lasciare alcun dubbio circa l'intenzione dell'interessato[262]. Quando riguarda il tratta- mento di dati sensibili, il consenso deve essere esplicito e può essere prestato oralmente o per iscritto[263]. A tale scopo possono essere utilizzati mezzi elettro- nici[264]. Nel quadro del diritto sia dell'UE sia del CdE, il consenso al trattamento dei dati personali deve essere dato mediante dichiarazione o atto positivo ine- quivocabile[265]. Pertanto, il consenso non può risultare dal silenzio, dalla prese- lezione di caselle, da moduli precompilati o dall'inattività[266].

L’articolo 5 del regolamento generale sulla protezione dei dati enuncia i principi che disciplinano il trattamento dei dati personali. Tali principi comprendono:

- liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza dei dati;
- limitazione della conservazione;

- integrità e riservatezza.

I principi fungono da punto di partenza per le disposizioni più dettagliate negli articoli successivi del regolamento. Essi figurano anche negli articoli 5, 7,
8 e 10 della Convenzione n. 108 modernizzata. Tutta la normativa seguente sulla tutela dei dati a livello del CdE o dell’UE deve rispettare questi principi, di cui occorre tener conto all’atto d’interpretare tale normativa. Nell’ambito del diritto dell’UE, le restrizioni ai principi relativi al trattamento dei dati sono ammesse solo nella misura in cui corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22 e devono rispettare il contenuto essenziale dei diritti e delle libertà fondamentali. Eventuali esenzioni e restrizioni riguardanti questi principi fondamentali possono essere previste a livello dell’UE o nazionale;[267]

devono essere previste per legge, perseguire un obiettivo legittimo e costituire misure necessarie e proporzionate in una società democratica.[268] Tutte e tre le condizioni devono essere soddisfatte:

3.1. Liceità, correttezza e trasparenza dei principi relativi al trattamento

- I principi di liceità, correttezza e trasparenza si applicano a tutti i trattamenti di dati personali.

- Ai sensi del RGPD, la liceità richiede la presenza di una delle seguenti condizioni:

- il consenso dell'interessato;

- la necessità di concludere un contratto;

- un obbligo legale;

- la necessità di salvaguardare gli interessi vitali dell'interessato o di un terzo;

- la necessità di eseguire un compito di interesse pubblico;

- la necessità di perseguire l'interesse legittimo del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi e i diritti dell'interessato.

- Il trattamento dei dati personali deve essere effettuato in modo corretto.

- L'interessato deve essere informato del rischio al fine di garantire che il trat- tamento non abbia effetti negativi imprevedibili.

- Il trattamento dei dati personali deve essere effettuato in modo trasparente.

- I titolari del trattamento devono informare gli interessati prima di elaborarne i dati, oltre ad altri dettagli, in merito alla finalità del trattamento e all'identità e all'indirizzo del titolare del trattamento.

- Le informazioni riguardanti le operazioni di trattamento devono essere for- nite utilizzando un linguaggio semplice e chiaro, affinché gli interessati pos- sano capire facilmente le norme, i rischi, le garanzie e i diritti in questione.

- Gli interessati hanno il diritto di accedere ai propri dati ovunque essi siano trattati.

3.1.1. Liceità del trattamento

La normativa dell'UE e del CdE in materia di protezione dei dati richiede che i dati personali siano trattati in modo lecito[269]. La liceità del trattamento richiede il consenso dell'interessato o un'altra base legittima prevista dalla legislazione in materia di protezione dei dati[270]. L'articolo 6, paragrafo 1, del RGPD prevede, oltre al consenso, cinque legittimi presupposti per il trattamento dei dati, ad esempio quando il trattamento dei dati personali è necessario per l'esecuzione di un contratto, per l'esecuzione di un compito connesso all'esercizio di pub- blici poteri, per adempiere un obbligo legale, per il perseguimento del legit- timo interesse del titolare del trattamento o di terzi, o se necessario per la sal- vaguardia degli interessi vitali dell'interessato. Questi aspetti sono trattati più dettagliatamente nella sezione 4.1.

3.1.2. Correttezza del trattamento

Oltre alla liceità del trattamento, la normativa dell'UE e del CdE in materia di protezione dei dati esige che i dati personali siano trattati in modo corretto[271]. Il principio di correttezza del trattamento disciplina principalmente la relazione tra il titolare del trattamento e l'interessato.

I responsabili del trattamento dei dati dovrebbero informare gli interessati e il pubblico in generale del fatto che tratteranno i dati in modo lecito e trasparente e devono essere in grado di dimostrare la conformità delle operazioni di trattamento con il RGPD. Le operazioni di trattamento non devono essere eseguite in segreto e gli interessati dovrebbero essere informati dei potenziali rischi. Inoltre, i responsabili del trattamento dei dati dovrebbero, per quanto possibile, agire in modo da conformarsi prontamente alla volontà dell'interessato, specialmente quando il suo consenso costituisce la base giuridica del trat- tamento dei dati.

Esempio: nella causa *K.H. e altri c. Slovacchia*[272], le ricorrenti erano donne di origine etnica rom che, durante la gravidanza e il parto, erano state ricoverate in due ospedali della Slovacchia orientale. Successivamente, nessuna di loro era stata in grado di concepire nuovamente un figlio, malgrado i ripetuti tentativi. I giudici nazionali avevano ordinato agli ospedali di permettere che le ricorrenti e i loro rappresentanti consultassero le cartelle cliniche annotando a mano degli estratti di informazioni, ma avevano respinto la richiesta di fotocopiare i documenti, presumibilmente al fine di evitare abusi. Tra gli obblighi degli Stati ai sensi dell'articolo 8 della CEDU era previsto necessariamente quello di mettere a disposizione degli interessati le copie dei propri fascicoli. Il compito di stabilire le modalità di copia dei fascicoli dei dati personali o, se del caso, di formulare motivi validi di rifiuto spettava allo Stato. Nel caso delle ricorrenti, i giudici nazionali avevano giustificato il divieto per le stesse di eseguire copie delle loro cartelle cliniche basandosi principalmente sulla necessità di proteggere le informazioni pertinenti da eventuali abusi. Tuttavia, la Corte EDU non ha ritenuto che le ricorrenti, alle quali era stato comunque accordato l'accesso a tutti i propri fascicoli medici, avrebbero potuto abusare delle informazioni che le riguardavano. Inoltre, il rischio di tale abuso avrebbe potuto essere evitato con mezzi diversi dal diniego del rilascio di copie dei fascicoli alle ricorrenti,

limitando per esempio le categorie di persone aventi diritto di accesso ai fascicoli. Lo Stato non è riuscito a dimostrare l'esistenza di motivi sufficientemente validi per negare alle ricorrenti l'accesso effettivo alle informazioni riguardanti la propria salute. La Corte ha concluso che vi era stata una violazione dell'articolo 8.

In relazione ai servizi Internet, le caratteristiche dei sistemi di trattamento dei dati devono essere tali da consentire agli interessati di comprendere realmente ciò che accade ai loro dati. In ogni caso, il principio di correttezza va al di là degli obblighi di trasparenza e potrebbe essere collegato anche al trattamento dei dati personali in maniera etica.

Esempio: un dipartimento di ricerca universitario conduce un esperimento analizzando i cambiamenti di umore su 50 soggetti. Questi ultimi sono tenuti a registrare i loro pensieri in un file elettronico ogni ora, in un dato momento. Le 50 persone hanno dato il loro consenso per questo particolare progetto e questo specifico uso dei dati da parte dell'università. Il dipartimento di ricerca scopre presto che la registrazione elettronica dei pensieri sarebbe

molto utile per un altro progetto, incentrato sulla salute mentale, coordinato da un'altra équipe. Anche se l'università, in quanto titolare del trattamento, avrebbe potuto utilizzare gli stessi dati per il lavoro di un'altra squadra, senza necessità di ulteriori misure volte a garantire la liceità del trattamento di tali dati, dal momento che le finalità sono compatibili, l'università ha informato i soggetti e chiesto un nuovo consenso, seguendo il proprio codice etico di ricerca e il principio della correttezza del trattamento.

3.1.3. Trasparenza del trattamento

La normativa dell'UE e del CdE in materia di protezione dei dati prescrive che i dati personali siano trat tati «in modo [...] trasparente nei confronti dell'interessato»[273].

Questo principio sancisce l'obbligo per il titolare del trattamento di adottare misure appropriate per tenere informati gli interessati (che potrebbero essere utenti, clienti o interlocutori) su come vengono utilizzati i loro dati[274]. La tra- sparenza può riferirsi alle informazioni fornite alla persona prima dell'inizio del trattamento[275], alle informazioni che devono essere facilmente accessibili agli interessati durante il trattamento[276], ma anche alle informazioni fornite

agli interessati a seguito di una richiesta di accesso ai dati che li riguardano[277].

Esempio: nella causa *Haralambie c. Romania*[278], il ricorrente aveva ottenuto l'accesso alle informazioni che lo riguardavano, conservate dall'organizzazione di servizi segreti, solo cinque anni dopo la sua richiesta. La Corte EDU ha ribadito che gli individui oggetto dei fascicoli personali tenuti dalle autorità pubbliche avevano un interesse vitale ad accedervi. Le autorità avevano il dovere di mettere a disposizione una procedura efficace per ottenere l'accesso a tali informazioni. La Corte EDU ha ritenuto che né la quantità di fascicoli trasmessi né le lacune del sistema di archivio giustificassero

un ritardo di cinque anni nell'accogliere la richiesta di accesso ai fascicoli presentata dal ricorrente. Le autorità non avevano messo a disposizione del ricorrente una procedura efficace e accessibile per consentirgli di ottenere l'accesso ai propri fascicoli personali entro un lasso di tempo ragionevole. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Le operazioni di trattamento devono essere illustrate agli interessati in modo facilmente comprensibile, affinché possano capire cosa accadrà ai loro dati. Ciò significa che la finalità specifica del trattamento dei dati personali deve essere conosciuta dall'interessato al momento della raccolta di detti dati personali[279]. La trasparenza del trattamento richiede che sia utilizzato un linguaggio sem- plice e chiaro[280]. Le persone interessate devono essere informate chiaramente sui rischi, sulle norme, sulle garanzie e sui diritti relativi al trattamento dei pro- pri dati personali[281].

Il diritto del CdE specifica, inoltre, che il titolare del trattamento deve obbli- gatoriamente fornire agli interessati, in maniera proattiva, determinate infor- mazioni essenziali. Le informazioni concernenti il nome e l'indirizzo del titolare (o dei contitolari) del trattamento, la base giuridica e le finalità del tratta- mento dei dati effettuato, le categorie di dati

trattati e i loro destinatari nonché i mezzi per esercitare i diritti, possono essere forniti in qualsiasi forma appro- priata (via un sito web, strumenti tecnologici o dispositivi personali, ecc.) a con- dizione che le informazioni siano presentate all'interessato in maniera corretta ed efficace. Le informazioni presentate devono essere facilmente accessibili, leggibili, comprensibili e adattate agli interessati (ad, esempio, in un linguaggio a misura di minori ove necessario). Deve altresì essere fornita qualsiasi altra informazione supplementare necessaria per garantire un trattamento dei dati corretto, o utile in tal senso, come la durata della conservazione dei dati, la conoscenza del ragionamento alla base del trattamento, o informazioni riguar- danti trasferimenti di dati verso un destinatario in un'altra parte o non parte (compreso se tale non parte offra o meno un livello di protezione adeguato,

o le misure adottate dal titolare del trattamento per garantire tale livello di protezione appropriato).[282]

In base al diritto di accesso[283], l'interessato ha il diritto di ottenere, a sua richie- sta, dal titolare del trattamento la conferma che sia o meno in corso un trat- tamento di dati che lo riguarda e in tal caso, di sapere quali dati sono soggetti a tale trattamento[284]. Inoltre, in base al diritto all'informazione[285], le persone i cui dati vengono trattati devono essere informati in maniera proattiva dai tito- lari o responsabili del trattamento circa le finalità, la durata, i mezzi di tratta- mento, oltre ad altri dettagli, in linea di principio prima dell'inizio dell'attività di trattamento.

Esempio: la causa *Smaranda Bara e a. c. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] riguardava la trasmissione di dati fiscali relativi al reddito di lavoratori autonomi dall'Agenzia nazionale per l'amministrazione tributaria alla Cassa nazionale malattia in Romania, sulla base dei quali veniva richiesto il pagamento di contributi per l'assicurazione malattia arretrati. Alla CGUE è stato chiesto di stabilire se l'interessato avrebbe dovuto ricevere informazioni preventive quanto all'identità del titolare del trattamento e all'obiettivo in vista del quale avveniva la

trasmissione dei dati, prima che tali dati fossero trattati dalla Cassa nazionale malattia. La CGUE ha stabilito che quando un'amministrazione pubblica di uno Stato membro trasmette dati personali a un'altra amministrazione pubblica che tratta ulteriormente tali dati, gli interessati devono essere informati di tale trasmissione o trattamento.

In determinate situazioni sono previste deroghe all'obbligo di informare gli interessati circa il trattamento dei dati; esse saranno approfondite nella sezione 6.1 sui diritti dell'interessato.

3.2. Il principio di limitazione della finalità

- La finalità del trattamento dei dati deve essere definita prima che il trattamento abbia inizio.

- Non può esservi ulteriore trattamento dei dati che non sia compatibile con la finalità iniziale, anche se il regolamento generale sulla protezione dei dati pre- vede eccezioni a questa regola a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica e a fini statistici.

- In sostanza, il principio della limitazione delle finalità significa che qualsiasi trat- tamento di dati personali deve essere effettuato per una finalità specifica e ben definita e solo per scopi ulteriori, specifici e compatibili con la finalità iniziale.

Il principio della limitazione della finalità è uno dei principi fondamentali del diritto europeo in materia di protezione dei dati. Esso è strettamente con- nesso con la trasparenza, la prevedibilità e il controllo dell'utente: se lo scopo del trattamento è sufficientemente specifico e chiaro, le persone sanno cosa aspettarsi e aumentano così la trasparenza e la certezza del diritto. Al tempo stesso, una chiara indicazione della finalità è

importante per consentire agli interessati di esercitare efficacemente i loro diritti, come il diritto di opposi- zione al trattamento[287].

In base a questo principio, il trattamento di dati personali deve essere effet- tuato per una finalità specifica e ben definita e solo per scopi ulteriori e compa- tibili con la finalità iniziale[288]. Il trattamento dei dati per finalità non definite e/o illimitate è, pertanto, illecito. È illecito anche il trattamento dei dati personali senza finalità certa, basato unicamente sulla considerazione che potrebbero essere utili in futuro. La liceità del trattamento di dati personali dipenderà dalla finalità del trattamento, che deve essere esplicita, specificata e legittima.

Ogni nuova finalità di trattamento dei dati che non sia compatibile con le fina- lità iniziali deve avere la propria base giuridica specifica e non può fondarsi sul fatto che i dati fossero stati inizialmente acquisiti o trattati per un'altra finalità

legittima. A sua volta, il trattamento lecito è limitato alla finalità iniziale spe- cificata per lo stesso e ogni nuova finalità di trattamento richiede una nuova base giuridica distinta. Per esempio, la divulgazione dei dati personali a terzi per una nuova finalità dovrà essere valutata con particolare attenzione, poiché tale divulgazione richiederà probabilmente un'altra base giuridica, distinta da quella prevista per la raccolta dei dati.

Esempio: una compagnia aerea raccoglie i dati dei passeggeri per effettuare le prenotazioni e quindi i voli correttamente. A tale scopo avrà bisogno di dati relativi a numeri di posto dei passeggeri, limitazioni fisiche specifiche, come la necessità di una sedia a rotelle, e richieste di pasti speciali, quali il cibo kosher o halal. Se alle compagnie aeree viene chiesto di trasmettere questi dati, contenuti nel codice di prenotazione, alle autorità preposte al controllo dell'immigrazione all'aeroporto di arrivo, si è in presenza di un utilizzo di tali dati per finalità di controllo dell'immigrazione, che differiscono dalla finalità della raccolta dei dati iniziale. La trasmissione di tali dati a un'autorità di controllo dell'immigrazione richiederà, pertanto, una base giuridica nuova e distinta.

Nel considerare l'ambito e i limiti di una particolare finalità, la Convenzione n. 108 modernizzata e il

regolamento generale sulla protezione dei dati ricor- rono al concetto di compatibilità: l'utilizzo dei dati per finalità compatibili è consentito in ragione della base giuridica iniziale. I dati non possono, pertanto, essere oggetto di un ulteriore trattamento considerato inatteso, inappropriato o contestabile dall'interessato[289]. Per accertare se un ulteriore trattamento sia da considerare compatibile, il titolare del trattamento dovrebbe tenere conto (tra l'altro):

- «di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto;

- del contesto in cui i dati personali sono stati raccolti, in particolare le ragio- nevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo;

- della natura dei dati personali;

• delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e

• dell'esistenza di garanzie adeguate sia nel trat tamento originario sia nell'ulteriore trattamento previsto»[290]. Ciò potrebbe essere realizzato, ad esempio, mediante la criptatura o la pseudonimizzazione dei dati.

Esempio: la società Sunshine acquisisce dati dei clienti in occasione della gestione dei rapporti con la clientela (CRM). Essa trasmette quindi i dati a u na società di vendita diretta, denominata Moonlight, che intende utilizzare questi dati per sostenere le campagne di promozione commercial e di aziende terze. La trasmissione di dati des tinati alla commercializzazione da par te di altre aziende costituisce trattamento successivo dei dati per una nuova finalità, incompatibile con la CRM, che è la finalità iniziale della società Sunshine per la raccolta dei dati dei clienti. La trasmissione dei dati alla società Moonlight necessita pertanto di una propria base giuridica.

Per contro, l'utilizzo dei dati nell'ambito della CRM della società Sunshine per le proprie finalità di promozione commerciale, ossia l'invio di messaggi di promozione commerciale ai propri clienti per i propri prodotti, è generalmente accettata come finalità compatibile.

Il regolamento generale sulla protezione dei dati e la Convenzione n. 108 modernizzata dichiarano che «[l]'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici» dovrebbe *a priori* essere considerato compatibile con la finalità iniziale[291]. Tuttavia, per l'ulteriore trattamento di dati personali devono essere previste garanzie adeguate, come l'anonimizzazione, la criptatura o la pseudonimizzazione dei dati e la limitazione dell'accesso ai dati[292]. Il regolamento generale

sulla protezione dei dati aggiunge che «[o]ve l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democra- tica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale, il titolare del trattamento dovrebbe poter sottoporre i dati perso- nali a ulteriore trattamento a prescindere dalla compatibilità delle finalità»[293]. Quando viene effettuato un ulteriore trattamento, l'interessato dovrebbe per- tanto essere informato delle finalità, nonché dei suoi diritti, compreso il diritto di opporsi[294].

Esempio: nell'ambito della gestione dei rapporti con la clientela (CRM), la società Sunshine ha raccolto e conservato i dati relativi ai propri clienti. L'utilizzo successivo di questi dati da par te della società Sunshine per un'analisi statistica delle abitudini di acquisto dei propri clienti è ammissibile, dal momento che le statistiche rappresentano una finalità compatibile. Non occorre alcuna base giuridica aggiuntiva, come il consenso degli interessati. Tuttavia, per l'ulteriore trattamento dei dati personali per finalità statistiche, la società Sunshine deve porre in essere garanzie appropriate per i diritti e le libertà dell'interessato. Le misure tecniche e organizzative che la società Sunshine deve attuare possono comprendere la pseudonimizzazione.

3.3. Il principio di minimizzazione dei dati

- Il trattamento dei dati deve essere limitato a quanto necessario per perseguire una finalità legittima.

- I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.

- Il trattamento dei dati non deve interferire in modo sproporzionato con gli inte- ressi, i diritti e le libertà in gioco.

Devono essere trattati solo i dati «adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successiva- mente trattati»[295]. Le categorie di dati scelte per il trattamento devono essere necessarie per conseguire l'obiettivo generale dichiarato delle operazioni di trattamento, e un titolare del trattamento dovrebbe limitare rigorosamente la raccolta di dati alle informazioni direttamente pertinenti per lo scopo specifico perseguito dal trattamento.

Esempio: nella causa *Digital Rights Ireland*[296], la CGUE ha considerato la validità della direttiva sulla conservazione dei dati, avente per obiettivo l'armonizzazione delle disposizioni nazionali relative alla conservazione di dati personali generati o trattati nell'ambito della fornitura di servizi o reti di comunicazione elettronica accessibili al pubblico, per la loro eventuale trasmissione alle autorità competenti a fini di perseguimento di reati gravi, come quelli legati alla criminalità organizzata e al terrorismo. Pur essendo considerata una finalità che risponde effettivamente a un obiettivo di interesse generale, il fatto che la direttiva riguardasse in maniera generale «qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi», è stato considerato problematico[297].

Inoltre, grazie all'utilizzo di tecnologie specifiche finalizzate a migliorare la tutela della vita privata, talvolta è possibile evitare del tutto l'utilizzo dei dati personali o utilizzare misure per ridurre la capacità di attribuire i dati all'inte- ressato (ad esempio, attraverso la pseudonimizzazione), offrendo una solu- zione rispet tosa della vita privata. Questo è par ticolarmente indicato nei sistemi di trattamento di portata più ampia.

Esempio: un consiglio comunale offre una tessera con microprocessore agli utenti abituali del sistema di trasporto pubblico cittadino dietro pagamento di un certo importo. Il nome dell'utente compare per iscritto sulla superficie della tessera e, in forma elettronica, nel microprocessore. A ogni corsa la

tessera dev’essere avvicinata all’apposito lettore installato, per esempio, sugli autobus e sui tram. I dati letti dal dispositivo sono controllati elettronicamente a fronte di quelli di una banca dati contenente i nomi delle persone che hanno acquistato la tessera di trasporto.

Questo sistema non rispetta appieno il principio di minimizzazione poiché il controllo della legittimità dell’uso dei mezzi di trasporto da parte di un individuo potrebbe essere effettuato senza confrontare i dati personali presenti sul microprocessore della tessera con quelli di una banca dati. Sarebbe sufficiente, per esempio, disporre di un’immagine elettronica particolare, come un codice a barre, nel microprocessore della tessera che, dopo essere stata avvicinata al lettore, confermerebbe o meno la validità della tessera. Un simile sistema non effettuerebbe alcuna registrazione di chi ha utilizzato un determinato mezzo di trasporto e a che ora. Questa sarebbe la soluzione ottimale ai sensi del principio di minimizzazione, che comporta l’obbligo di minimizzare la raccolta dei dati.

L’articolo 5, paragrafo 1, della Convenzione n. 108 modernizzata, contiene un requisito di proporzionalità per il trattamento dei dati personali in relazione allo scopo legittimo perseguito. Deve sussistere un giusto equilibrio fra tutti gli interessi in gioco, in tutte le fasi del trattamento. Questo

significa che «[d]ati personali che sarebbero adeguati e pertinenti, ma implicherebbero un’ingerenza sproporzionata nei diritti e nelle libertà fondamentali in gioco, devono essere considerati eccessivi»[298].

3.4. Il principio di esattezza dei dati

- Il principio di esattezza dei dati deve essere attuato dal titolare del trattamento in tutte le operazioni di trattamento.

- I dati inesatti devono essere cancellati o rettificati tempestivamente.

- Può essere necessario controllare i dati regolarmente e costantemente, aggior- nandoli per garantirne l’esattezza.

Un titolare del trattamento in possesso di informazioni personali non deve uti- lizzare tali informazioni senza adottare misure volte a garantire con ragione- vole certezza che i dati siano esatti e aggiornati[299].

L'obbligo di garantire l'esattezza dei dati deve essere visto nel contesto della finalità del trattamento dei dati.

Esempio: nella causa *Rijkeboer*[300], la CGUE ha preso in esame la richiesta di un cittadino olandese all'amministrazione comunale della città di Amsterdam, di informare lo stesso circa l'identità delle persone alle quali l'amministrazione comunale aveva trasmesso nei due anni precedenti informazioni che lo riguardavano, nonché il contenuto dei dati comunicati. La CGUE ha dichiarato che il «diritto al rispetto della vita privata implica che la persona interessata possa assicurarsi che i suoi dati personali siano trattati in modo corretto e lecito, vale a dire, in particolare, che i dati di base che la riguardano siano corretti e vengano inviati a destinatari autorizzati». La CGUE ha quindi fatto riferimento al preambolo della direttiva sulla protezione dei dati, che afferma che gli interessati devono godere del diritto di accesso ai propri dati personali per poter verificare la loro esattezza[301].

Possono presentarsi anche casi in cui l'aggiornamento dei dati archiviati è proi- bito per legge, perché la finalità della conservazione dei dati è principalmente quella di documentare eventi come uno «scatto storico».

Esempio: una cartella clinica riguardante un intervento non deve essere modificata, in altre parole «aggiornata», anche se in un secondo momento risulta che le conclusioni ivi riportate erano errate. In tali circostanze, possono essere effettuate solo aggiunte alle note della cartella medica, purché siano chiaramente indicate come elementi apportati in una fase successiva.

D'altra parte, vi sono situazioni in cui il controllo regolare dell'esattezza dei dati, fra cui l'aggiornamento, costituisce una necessità assoluta a causa del potenziale danno per l'interessato qualora i dati dovessero rimanere inesatti.

Esempio: se un soggetto intende stipulare un contratto di finanziamento con un istituto bancario, la banca generalmente controllerà l'affidabilità creditizia del potenziale cliente. A tal fine, sono disponibili banche dati specifiche contenenti i dati sullo storico creditizio dei privati. Se tale banca dati fornisce dati errati o non aggiornati riguardanti un individuo, questa persona può subire effetti negativi. Pertanto, i titolari del trattamento di tali banche dati devono adoperarsi in modo specifico per rispettare il principio di esattezza.

3.5. Il principio della limitazione della conservazione

- Il principio della limitazione della conser vazione significa che i dati personali devono essere cancellati o anonimizzati non appena questi non siano più neces- sari alle finalità per cui sono stati raccolti.

L'articolo 5, paragrafo 1, lettera e), del RGPD, nonché l'articolo 5, paragrafo 4, lettera e) della Convenzione n. 108 modernizzata, esigono che i dati perso- nali siano «conservati in una forma che consenta l'identificazione degli inte- ressati per un arco di tempo non superiore al conseguimento delle

finalità per le quali sono trattati». Pertanto, i dati devono essere cancellati o anonimizzati quando tali finalità sono state soddisfatte. A tal fine, «il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica», per garantire che i dati non siano conservati più a lungo del necessario[302].

Nella causa *S. e Marper*, la Corte EDU ha concluso che i principi fondamentali degli strumenti pertinenti del Consiglio d'Europa nonché del diritto e della prassi in vigore presso le altre parti contraenti richiedevano che la conserva- zione dei dati fosse proporzionata allo scopo per il quale essi sono raccolti e avere una durata limitata nel tempo, in particolare nel settore della polizia[303].

Esempio: nella causa *S. e Marper*[304], la Corte EDU ha stabilito che la conservazione per una durata indeterminata delle impronte digitali, dei campioni cellulari e dei profili di DNA dei due ricorrenti era sproporzionata e non necessaria in una società democratica, considerando che le azioni penali promosse contro entrambi i ricorrenti si erano concluse con l'assoluzione e il non luogo a procedere, rispettivamente.

I limiti di tempo per la conservazione dei dati personali si applicano solo ai dati conservati in un formato che consenta l'identificazione degli interessati. La conservazione legittima dei dati che non sono più necessari potrebbe essere dunque ottenuta attraverso l'anonimizzazione degli stessi.

I dati archiviati a fini di interesse pubblico, ricerca scientifica o storica o usi sta- tistici, possono essere conservati per periodi più lunghi, a condizione che siano utilizzati esclusivamente per le finalità di cui sopra[305]. Devono essere adottate misure tecniche e organizzative adeguate per la conservazione e l'uso continui dei dati personali, al fine di salvaguardare i diritti e le libertà dell'interessato.

Anche la Convenzione n. 108 modernizzata permette eccezioni al principio di limitazione della conservazione, a condizione che siano previste per

legge, rispet tino il contenuto essenziale dei diritti e delle liber tà fondamentali e siano necessarie e proporzionate per perseguire un numero limitato di obiet- tivi legittimi[306]. Tra questi vi sono, tra l'altro, la tutela della sicurezza nazio- nale, l'indagine e il perseguimento di reati, l'esecuzione di sanzioni penali, la tutela dell'interessato e la protezione dei diritti e delle libertà fondamentali altrui.

Esempio: nella causa *Digital Rights Ireland*[307], la CGUE ha esaminato la validità della direttiva sulla conservazione dei dati, avente per obiettivo l'armonizzazione delle disposizioni nazionali relative alla conservazione di dati personali generati o trattati nell'ambito della fornitura di servizi o reti di comunicazione elettronica accessibili al pubblico a fini di perseguimento di

reati gravi, come quelli legati alla criminalità organizzata e al terrorismo. La direttiva sulla conservazione dei dati imponeva un periodo di conservazione dei dati di «almeno sei mesi senza che [venisse] effettuata alcuna distinzione tra le categorie di dati previste all'articolo 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate»[308]. La CGUE ha altresì sollevato il problema della mancanza di criteri oggettivi nella direttiva sulla conservazione dei dati, sulla base dei quali determinare la durata esatta di conservazione (che potrebbe variare tra un minimo di sei mesi ad un massimo di 24 mesi) al fine di garantire che tale periodo sia limitato a quanto strettamente necessario[309].

3.6. Il principio della sicurezza dei dati

- La sicurezza e la riservatezza dei dati personali sono fondamentali per prevenire effetti negativi per l'interessato.

- Le misure di sicurezza possono essere di natura tecnica e/o organizzativa.

- La pseudonimizzazione è un processo che può proteggere i dati personali.

- L’adeguatezza delle misure di sicurezza deve essere determinata caso per caso e valutata periodicamente.

Il principio di sicurezza dei dati richiede che, nel trattare dati personali, siano messe in atto misure tecniche o organizzative adeguate per proteggere i dati da accesso, uso, modifica, divulgazione, perdita, distruzione o danno acci- dentali, non autorizzati o illegali.[310] Il RGPD prevede che, nell’attuazione di tali misure, il titolare del trattamento e il responsabile del trattamento, ten- gano conto «dello stato dell’arte e dei costi di at tuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche»[311]. A seconda delle circostanze specifiche di ciascun caso, le misure

tecniche adeguate potrebbero comprendere, ad esempio, la pseudonimizza- zione e la cifratura dei dati personali e/o testare e valutare regolarmente l'effi- cacia delle misure per garantire la sicurezza del trattamento dei dati[312].

Come illustrato nella sezione 2.1.1, pseudonimizzare i dati significa sostituire con uno pseudonimo gli attributi, contenuti nei dati personali, che consentono di identificare l'interessato, e conservare tali attributi separatamente, sulla base di misure tecniche o organizzative. Il processo di pseudonimizzazione non deve essere confuso con il processo di anonimizzazione, in cui viene spezzato ogni nesso che permette l'identificazione della persona.

Esempio: la frase «Charles Spencer, nato il 3 aprile 1967, è padre di quattro figli, due maschi e due femmine» può essere pseudonimizzata come segue:

«C.S. 1967 è padre di quattro figli, due maschi e due femmine», o

«324 è padre di quattro figli, due maschi e due femmine», o

«YESz320l è padre di quattro figli, due maschi e due femmine».

Solitamente, gli utenti che accedono ai dati pseudonimizzati non hanno alcuna possibilità d'identificare "Charles Spencer, nato il 3 aprile 1967" con "324" o "YESz3201". Pertanto è più probabile che tali dati non siano esposti a un uso improprio.

Il primo esempio è tuttavia meno sicuro. Se la frase «C.S 1967 è padre di quat- tro figli, due maschi e due femmine» è utilizzata nel paesino dove vive Charles Spencer, il sig. Spencer può essere facilmente riconoscibile. Il metodo di pseu- donimizzazione può incidere sull'efficacia della protezione dei dati.

I dati personali con attributi cifrati o conservati separatamente sono utilizzati in molti contesti per mantenere segreta l'identità delle persone. Ciò si rivela par ticolarmente utile quando i titolari del trat tamento devono accer tarsi che si tratti dello stesso interessato, ma non necessitano, o non dovrebbero disporre, dell'identità reale dell'interessato. È il caso, per esempio, di un ricer- catore che studia il decorso di una malattia in pazienti la cui identità è nota

solo alla struttura ospedaliera in cui questi sono trattati e dalla quale il ricerca- tore ottiene le anamnesi in versione pseudonimizzata. La pseudonimizzazione costituisce quindi una solida pratica nel novero delle tecnologie intese a miglio- rare la tutela della vita privata. Può fungere da elemento importante per rea- lizzare la tutela della vita privata fin dalla progettazione, ossia per integrare la protezione dei dati nei sistemi avanzati di trattamento dei dati.

L'articolo 25 del RGPD, che riguarda la protezione dei dati fin dalla progetta- zione, fa esplicito riferimento alla pseudonimizzazione come esempio di misura tecnica e organizzativa adeguata, che i titolari del trattamento dovrebbero mettere in atto per rispettare i principi di protezione dei dati e per integrare le necessarie garanzie. In tal modo, i titolari del trattamento potranno soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, quando trattano i dati personali di questi ultimi.

L'adesione a un codice di condotta approvato o a un meccanismo di certifica- zione approvato può contribuire a dimostrare la conformità al requisito della sicurezza del trattamento[313]. Nel suo parere sulle implicazioni della protezione dei dati nel trattamento dei dati del codice di prenotazione dei passeggeri, il Consiglio d'Europa fornisce altri esempi di misure di sicurezza appropriate per la protezione dei dati personali nei sistemi di codici di

prenotazione, come la conservazione dei dati in un ambiente fisico sicuro, la limitazione del controllo degli accessi mediante autenticazioni separate e la tutela della comunicazione dei dati utilizzando una crittografia avanzata[314].

Esempio: i siti di social networking e i fornitori di posta elettronica consentono agli utenti di aggiungere un ulteriore livello di sicurezza dei dati per i servizi che forniscono, attraverso l'introduzione dell'autenticazione a due livelli. Oltre a inserire una parola d'accesso personale, gli utenti devono completare una seconda autenticazione, per accedere al proprio account personale. Quest'ultimo potrebbe consistere, per esempio, nell'immissione di un codice di sicurezza inviato al numero di cellulare collegato al conto personale.

In questo modo, la verifica in due fasi fornisce una migliore protezione delle informazioni personali dall'accesso non autorizzato a conti personali attraverso atti di pirateria.

La relazione esplicativa della Convenzione n. 108 modernizzata fornisce ulteriori esempi di garanzie adeguate, quali l'introduzione dell'obbligo del segreto profes- sionale o l'adozione di misure tecniche di sicurezza qualificate, quali la cifratura dei dati[315]. Quando attua misure di sicurezza specifiche, il titolare del trattamento o, ove pertinente, il responsabile del trattamento, deve tenere conto di diversi elementi, quali la natura e il volume dei dati personali trattati, le potenziali con- seguenze negative per gli interessati e la necessità di limitare l'accesso ai dati[316]. Nell'attuazione di misure di sicurezza adeguate, devono essere tenuti in consi- derazione gli attuali metodi e tecniche allo stato dell'arte in materia di sicurezza nell'ambito del trattamento dei dati. Il costo di tali misure deve essere proporzio- nato alla gravità e alla probabilità dei rischi potenziali. Una valutazione periodica delle misure di sicurezza è necessaria affinché possano essere aggiornate, ove necessario[317].

In caso di violazione di dati personali, sia la Convenzione n. 108 modernizzata sia il RGPD richiedono al titolare del trattamento di notificare, senza ingiusti- ficato ritardo, all'autorità di controllo

competente, la violazione che presenti un rischio per i diritti e le libertà delle persone fisiche[318]. Un obbligo simile di comunicazione all'interessato sussiste quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle per- sone fisiche[319]. La comunicazione di tali violazioni agli interessati deve essere formulata in un linguaggio semplice e chiaro[320]. Se il responsabile del tratta- mento viene a conoscenza di una violazione dei dati personali, il titolare del trattamento deve esserne informato immediatamente[321]. In determinate situa- zioni, all'obbligo di notifica possono applicarsi eccezioni. Per esempio, il titolare

del trattamento non è tenuto a notificare l'autorità di controllo quando «sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche»[322]. Né è necessario notificare l'interessato quando le misure di sicurezza applicate rendono i dati personali incomprensibili alle persone non autorizzate o quando misure successive scongiurano il soprag- giungere di un rischio elevato[323]. Se la comunicazione di una violazione dei dati personali agli interessati richiede sforzi sproporzionati da parte del titolare del trattamento, una comunicazione pubblica o una misura simile può garantire che «gli interessati [siano] informati con analoga efficacia»[324].

3.7. Il principio di responsabilizzazione

- La responsabilizzazione richiede da parte dei titolari e dei responsabili del tratta- mento di adottare attivamente e in modo permanente misure finalizzate alla pro- mozione e alla salvaguardia della protezione dei dati nelle attività di trattamento.

- I titolari e i responsabili del trattamento sono responsabili della conformità alla normativa in

materia di protezione dei dati nell'ambito delle operazioni di tratta- mento e dei rispettivi obblighi.

• I titolari del trat tamento devono essere in g rado di dimostrare in qualsiasi momento agli interessati, al pubblico in generale e alle autorità di controllo che essi operano in conformità delle disposizioni sulla protezione dei dati. I responsa- bili del trattamento devono altresì rispettare alcuni obblighi strettamente legati alla responsabilità (ad esempio, tenere un registro delle attività di trattamento e designare il responsabile della protezione dei dati).

Il RGPD e la Convenzione n. 108 modernizzata stabiliscono che il titolare del trattamento è competente per il rispetto dei principi di trattamento dei dati personali descritti in questo capitolo e deve essere in grado di comprovarlo[325]. A tale scopo, il titolare del trattamento deve mettere in atto misure tecni- che e organizzative adeguate[326]. Sebbene il principio di responsabilizzazione di cui all'articolo 5, parag rafo 2, del RGPD sia rivolto solo ai titolari del

trattamento, anche i responsabili del trattamento sono da ritenersi competenti, dal momento che devono ottemperare a diversi obblighi e che sono stretta- mente collegati alla responsabilità.

La normativa dell'UE e del CdE in materia di protezione dei dati stabilisce altresì che il titolare del trattamento è competente per il rispetto dei principi di pro- tezione dei dati illustrati nelle sezioni da 3.1 a 3.6, e deve essere in grado di comprovarlo[327]. Il Gruppo articolo 29 per la tutela dei dati sottolinea che «il tipo di procedure e di meccanismi varierebbe in funzione dei rischi intrinseci al trat- tamento e alla natura dei dati»[328].

I titolari del trattamento possono facilitare il rispetto di questo requisito in diversi modi, tra cui:

- tenere un registro delle attività di trattamento e, su richiesta, metterlo a disposizione dell'autorità di controllo[329];

- in determinate situazioni, designare il responsabile della protezione dei dati, che è coinvolto in tutte le questioni connesse alla protezione dei dati personali[330];

- svolgere valutazioni d'impatto sulla protezione dei dati per i tipi di tratta- mento che

presentano un rischio elevato per i diritti e le libertà delle per- sone fisiche[331];

- garantire la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita[332];

- prevedere modalità e procedure per l'esercizio dei diritti degli interessati[333];

- aderire a codici di condotta approvati o a meccanismi di certificazione[334].

Pur non essendo il principio di responsabilizzazione di cui all’articolo 5, para- grafo 2, del RGPD, specificamente rivolto ai responsabili del trattamento, esi- stono disposizioni connesse alla responsabilità, che contengono anche obblighi riguardanti questi ultimi, come tenere un registro delle attività di trattamento e designare il responsabile della protezione dei dati per le attività di trattamento che lo richiedono[335]. I responsabili del trattamento devono altresì assicurare l’adozione di tutte le misure richieste per garantire la sicurezza dei dati[336]. Il contratto giuridicamente vincolante tra il titolare del trattamento e il respon- sabile del trattamento deve prevedere che il responsabile assista il titolare con riferimento al rispetto di alcuni obblighi, ad esempio nello svolgimento di una valutazione d’impatto sulla protezione dei dati o quando notifica al titolare del trattamento eventuali violazioni non appena ne viene a conoscenza[337].

Nel 2013 l’Organizzazione per la cooperazione e lo sviluppo economici (OCSE) ha adottato alcuni orientamenti sulla vita privata in cui si sottolinea l’importante ruolo dei titolari del trattamento nell’attuazione concreta della protezione dei dati. Gli orientamenti comprendono il principio di responsabilizzazione nel senso che «un titolare del trattamento dovrebbe essere responsabile del rispetto delle misure che danno attuazione ai principi (materiali) sopra enunciati»[338].

Esempio: un esempio legislativo che sottolinea il principio di responsabi- lizzazione è costituito dalla modifica[339] della direttiva e-privacy 2002/58/CE, avvenuta nel 2009. Ai sensi dell'articolo 4 della versione modificata, la direttiva prevede l'obbligo di «[garantire] l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali». Così, per quanto riguarda le disposizioni di sicurezza di tale direttiva, il legislatore ha deciso che era necessario introdurre l'obbligo esplicito di predisporre e attuare una politica di sicurezza.

Secondo il parere del Gruppo di lavoro articolo 29[340], la componente essenziale della responsabilità è data dall'obbligo del titolare del trattamento di:

- mettere in atto misure per garantire – in circostanze normali – che le norme in materia di protezione dei dati siano rispettate nel contesto delle opera- zioni di trattamento e

- disporre di documentazione atta a dimostrare agli interessati e alle auto- rità di controllo le misure adottate per conseguire il rispetto delle norme in materia di protezione dei dati.

Il principio di responsabilizzazione esige quindi che i titolari del trattamento ne dimostrino attivamente il rispetto, senza limitarsi ad aspettare che gli interes- sati o le autorità di controllo sottolineino eventuali carenze.

I principi sono necessariamente di natura generale. La loro applicazione a situ- azioni concrete lascia un certo margine di interpretazione e di scelta dei mezzi. Il diritto del CdE consente alle parti aderenti alla Convenzione n. 108 moderniz- zata di chiarire questo margine d’interpretazione nel rispettivo diritto nazionale. La situazione nel diritto dell’UE è diversa: per instaurare la protezione dei dati nel mercato interno si è ritenuto necessario disporre di norme più dettagliate a livello dell’UE, al fine di armonizzare il grado di protezione dei dati previsto dalle legislazioni nazionali degli Stati membri. Il regolamento generale sulla pro- tezione dei dati stabilisce, secondo i principi di cui all’articolo 5, un corpus di norme dettagliate che sono direttamente applicabili nell’ordinamento giuridico nazionale. Le seguenti osservazioni riguardanti le norme dettagliate in materia di protezione dei dati a livello europeo riguardano, pertanto, prevalentemente il diritto dell’UE.

4.1. Norme sulla liceità del trattamento

- I dati personali possono essere trattati in modo lecito se è soddisfatto uno dei seguenti criteri:

- il trattamento si basa sul consenso dell'interessato;

- un rapporto contrattuale richiede il trattamento di dati personali;

- il trattamento è necessario per adempiere un obbligo legale al quale è sog- getto il titolare del trattamento;

- gli interessi vitali degli interessati o di altri richiedono il trattamento dei loro dati;

- il trattamento è necessario all'esecuzione di un compito di interesse pubblico;

- gli interessi legittimi dei responsabili del trattamento dei dati, o di terzi, costi- tuiscono il motivo del trattamento, ma solo a condizione che non prevalgano gli interessi o i diritti fondamentali degli interessati.

• La liceità del trattamento dei dati personali sensibili è soggetta a un regime par- ticolare e più rigoroso.

4.1.1. Legittimi presupposti per il trattamento dei dati

Il capo II del regolamento generale sulla protezione dei dati, intitolato «Prin- cipi», stabilisce che qua lsiasi trat tamento di dati perso na li deve essere conforme, in primo luogo, ai principi relativi alla qualità dei dati previsti dall'articolo 5 del RGPD. Uno dei principi è che i dati personali devono essere «trattati in modo lecito, corretto e trasparente» In secondo luogo, affinché i dati siano trattati in modo lecito, il trattamento deve essere conforme a uno dei legittimi presupposti per il trattamento dei dati, elencati all'articolo 6[341] per i dati personali non sensibili, e all'articolo 9, per le categorie particolari di dati (o dati sensibili). In modo analogo, il capitolo II della Convenzione n. 108 modernizzata, che definisce i «principi fondamentali per la protezione dei dati

personali», stabilisce che, per essere lecito, il trattamento dei dati deve essere «proporzionato allo scopo legittimo perseguito».

Indipendentemente dal legittimo presupposto per il trattamento dei dati, sul quale il titolare del trattamento si basa per avviare un'operazione di tratta- mento dei dati personali, il titolare dovrà anche applicare le garanzie previste dal regime generale del diritto in materia di protezione dei dati.

Consenso

Nell'ambito del diritto del CdE, il consenso è menzionato nell'articolo 5, paragrafo 2, della Convenzione n. 108 modernizzata. È altresì citato nella giurisprudenza della Corte EDU e in diverse raccomandazioni del Consiglio d'Europa[342]. Nell'ambito del diritto dell'UE, il consenso come base per il trat- tamento lecito dei dati è sancito con fermezza nell'articolo 6 del RGPD ed è altresì esplicitamente richiamato nell'articolo 8 della Car ta. Le carat teris- tiche per un valido consenso sono illustrate nella definizione di consenso di cui all'articolo 4, mentre le condizioni per ottenere un valido consenso sono descritte in dettaglio all'articolo 7 e le norme particolari per il consenso dei minori in relazione ai ser vizi della società dell'informazione sono stabilite nell'articolo 8 del RGPD.

Come spiegato nella sezione 2.4, il consenso deve essere libero, informato, specifico e inequivocabile. Esso deve essere una dichiarazione o un atto positivo e inequivocabile di accettazione del trattamento, e la persona ha il diritto di revocare il proprio consenso in qualsiasi momento. I titolari del trattamento hanno il dovere di tenere un'evidenza verificabile del consenso.

Libero consenso

Nel quadro del CdE, ai sensi della Convenzione n. 108 modernizzata, il con- senso dell'interessato deve «rappresentare la libera espressione di una scelta intenzionale»[343]. Il libero consenso è valido «soltanto se l'interessato è in grado di operare realmente una scelta, e non c'è il rischio di raggiri, intimidazioni,

coercizioni o conseguenze negative significative nel caso in cui questa persona non manifesti il proprio consenso»[344]. In tal senso, il diritto dell'UE stabilisce che il consenso non è considerato liberamente espresso «se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio»[345]. Il RGPD sottolinea che «[n]el valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto»[346]. La relazione esplicativa della Convenzione n. 108 moderniz- zata dichiara che [n]essuna influenza o pressione indebita (di natura economica o altro), diretta o indiretta, può essere esercitata sull'interessato e il consenso non deve essere considerato come liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio[347].

Esempio: alcuni comuni dello Stato A hanno deciso di realizzare tessere di soggiorno con un microprocessore incorporato. I residenti non hanno l'obbligo di acquistare tali tessere elettroniche. Tuttavia, i residenti che non sono in possesso della

tessera non hanno accesso a una serie di importanti servizi amministrativi, quali la possibilità di pagare le imposte comunali on-line, presentare reclami per via elettronica beneficiando di un termine di tre giorni entro i quali l'autorità è tenuta a rispondere, nonché evitare code, acquistare biglietti a prezzo ridotto per visitare la sala concerti comunale e utilizzare gli scanner all'ingresso.

In questo esempio, il trattamento dei dati personali da parte dei comuni non può essere basato sul consenso. Dal momento che i residenti subiscono come minimo una pressione indiretta per ottenere la tessera elettronica e acconsentire al trattamento, il consenso non è espresso liberamente. La realizzazione da parte dei comuni di un sistema di tessere elettroniche dovrebbe, pertanto, basarsi su un altro motivo legittimo che giustifichi il

trattamento. Per esempio, potrebbero invocare la necessità del trattamento per l'esecuzione di un compito svolto nell'interesse pubblico, che è una base legittima per il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera e), del RGPD[348].

Il libero consenso potrebbe anche essere messo in dubbio in situazioni di sub- ordinazione, in cui vi è un significativo squilibrio economico o di altro tipo tra il titolare del trattamento che acquisisce il consenso e l'interessato che lo for- nisce[349]. Un tipico esempio di tali squilibri e subordinazione è il trattamento di dati personali da parte del datore di lavoro, nel contesto di un rapporto di lavoro. Secondo il Gruppo di lavoro articolo 29, «[i] dipendenti non sono quasi mai in condizione di esprimere liberamente, rifiutare o revocare il consenso, a causa della dipendenza che deriva dal rapporto datore di lavoro/dipendente. Dato lo squilibrio di potere, i dipendenti possono esprimere il libero consenso solo in circostanze eccezionali, quando all'accettazione o al rifiuto di un'offerta non è collegata nessuna conseguenza»[350].

Esempio: una grande società prevede di creare un repertorio contenente i nomi di tutti i dipendenti, la loro funzione in seno alla società e i loro indirizzi aziendali, esclusivamente per migliorare le comunicazioni interne della società. Il responsabile

del personale propone di aggiungere una foto di ciascun dipendente al repertorio, per rendere più facile il riconoscimento dei colleghi durante le riunioni. I rappresentanti dei dipendenti chiedono che questo sia fatto soltanto con il consenso di ciascun dipendente.

In questo caso, il consenso di un dipendente dovrebbe essere riconosciuto come la base giuridica per il trattamento delle foto nel repertorio,

perché è credibile che il dipendente non andrà incontro a conseguenze, a prescindere che decida per la pubblicazione o meno di tale foto nel repertorio.

Esempio: la società A sta pianificando una riunione fra tre dei suoi dipendenti e i dirigenti della società B per discutere di una potenziale futura cooperazione a un progetto. La riunione si svolgerà presso la sede della società B, che chiede alla società A di inviare loro, via e-mail, nomi, curriculum vitae e foto dei partecipanti alla riunione. La società B afferma di avere bisogno dei nomi e delle foto dei partecipanti per consentire al personale di sicurezza all’ingresso dell’edificio di verificare che si tratti delle persone giuste, mentre il curriculum vitae ha lo scopo di consentire all’amministrazione di prepararsi meglio alla riunione. In questo caso, la trasmissione, da parte della società A, dei dati personali dei propri dipendenti non può basarsi sul consenso. Il consenso non potrebbe considerarsi «liberamente prestato», dal momento che è possibile che i dipendenti debbano affrontare conseguenze negative se rifiutano l’offerta (ad esempio, potrebbero essere sostituiti da un altro collega, non solo nella partecipazione alla riunione, ma anche per quanto riguarda le relazioni con la società B e la partecipazione al progetto in generale). Pertanto, il trattamento deve basarsi su un altro legittimo presupposto che lo giustifichi.

Ciò non significa, tuttavia, che il consenso non possa mai essere valido in cir- costanze in cui il mancato consenso avrebbe alcune conseguenze negative. Se, per esempio, il mancato consenso a ricevere la carta clienti di un supermer- cato ha come conseguenza solo il fatto di non ottenere una piccola riduzione del prezzo di determinati prodotti, il consenso potrebbe costituire una valida base giuridica per il trattamento dei dati personali di quei clienti che hanno acconsentito ad avere tale carta. Non vi è alcuna situazione di subordinazi- one tra azienda e cliente e le conseguenze del mancato consenso non sono abbastanza gravi per l'interessato da impedire la libera scelta (a condizione che la riduzione del prezzo sia sufficientemente ridotta da non influire sulla libera scelta).

D'altra parte, quando prodotti o servizi possono essere ottenuti solo se alcuni dati personali sono comunicati al titolare del trattamento o successivamente a terzi, il consenso dell'interessato alla divulgazione dei propri dati, che non siano necessari all'esecuzione del contratto, non può essere considerato frutto di una decisione libera ed è, quindi, non valido ai sensi del diritto in materia di

protezione dei dati[351]. Il RGPD è piuttosto rigido nel proibire l'integrazione del consenso con la fornitura di prodotti e servizi[352].

Esempio: l'accordo espresso dai passeggeri di una compagnia aerea che trasmette i cosiddetti codici di prenotazione (ovvero i dati riguardanti la loro identità, abitudini alimentari o problemi di salute) alle autorità competenti per l'immigrazione di un paese straniero specifico non può essere considerato un valido consenso ai sensi del diritto in materia di protezione dei dati, dato che i passeggeri in viaggio non hanno scelta se vogliono visitare questo paese. Se tali dati devono essere trasmessi legittimamente, è richiesta una base giuridica diversa dal consenso, ossia molto probabilmente una legge specifica.

Consenso previa informazione

L'interessato deve disporre di informazioni sufficienti prima di esercitare la sua scelta. Il consenso previa informazione comprende di solito una descrizione precisa e facilmente comprensibile della materia rispetto alla quale è rich- iesto consenso. Come illustrato dal Gruppo di lavoro articolo 29, il consenso deve essere basato su un apprezzamento e sulla comprensione dei fatti e delle implicazioni dell'azione della persona interessata per il consenso al trat- tamento. Pertanto, «[l]'interessato deve

ricevere, in modo chiaro e compren- sibile, informazioni precise e complete su tutti gli aspetti rilevanti [...], come la natura dei dati trattati, le finalità del trattamento, i destinatari di eventuali trasferimenti e i diritti dell'interessato»[353]. Affinché il consenso sia prestato con cognizione di causa, le persone devono altresì essere consapevoli delle con- seguenze del mancato consenso al trattamento.

In considerazione dell'importanza del consenso previa informazione, il RGPD e la relazione illustrativa della Convenzione n. 108 modernizzata hanno cer- cato di chiarire la nozione. I considerando del RGPD stabiliscono che «[a]i fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza

almeno dell’identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali»[354].

Nel caso eccezionale del consenso utilizzato come deroga per assicurare un legittimo presupposto per un trasferimento di dati internazionale, affinché il consenso sia considerato valido, il titolare del trattamento deve informare l’interessato dei possibili rischi di siffatto trasferimento, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate[355].

La relazione esplicativa della Convenzione n. 108 modernizzata precisa che l’interessato deve essere informato circa le implicazioni della sua decisione, e precisamente «cosa significa il fatto di prestare il proprio consenso e la misura dello stesso»[356].

La qualità dell’informazione è importante. Qualità dell’informazione significa che il linguaggio della stessa dovrebbe essere adattato ai prevedibili desti- natari. Le informazioni devono essere fornite mediante un linguaggio privo di espressioni gergali, che sia chiaro e comprensibile a un utente medio[357]. Esse devono altresì essere facilmente accessibili all’interessato e possono essere fornite oralmente o per iscritto. L’accessibilità e la visibilità delle informazioni sono fattori importanti: l’informazione deve essere chiara e ben visibile. In un ambiente online, la disponibilità di informative su

più livelli può rappresentare una buona soluzione, in quanto esse consentono all'interessato di scegliere se accedere a una versione sintetica delle informazioni o a una versione più dettagliata.

Consenso specifico

Per essere valido, il consenso deve essere anche specifico alla finalità del trat- tamento, che deve essere descritta in modo chiaro e in termini inequivocabili. Questa caratteristica va di pari passo con la qualità delle informazioni fornite circa la finalità del consenso. In questo contesto, sarà pertinente ciò che un

interessato medio ragionevolmente si aspetta in termini di oggetto del con- senso. All’interessato deve essere chiesto nuovamente il consenso se devono essere effettuate operazioni di trattamento aggiuntive o se queste devono essere modificate in un modo che non poteva ragionevolmente essere previsto quando è stato dato il consenso iniziale, traducendosi così in un cambiamento di finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste[358].

Esempi: nella causa *Deutsche Telekom AG*[359], la CGUE ha affrontato la questione se un provider di servizi di telecomunicazione, che doveva trasmettere i dati personali degli abbonati affinché fossero pubblicati in elenchi, necessitasse nuovamente del consenso degli interessati[360], in quanto inizialmente, quando era stato dato il consenso, non erano stati specificati i destinatari dei dati.

La CGUE ha ritenuto che, ai sensi dell’articolo 12 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, non fosse necessario un nuovo consenso prima di trasmettere i dati. Dal momento che avevano la possibilità di acconsentire solo alla finalità del trattamento (che era la pubblicazione dei loro dati), gli interessati non potevano scegliere tra diversi elenchi in cui tali dati potevano essere pubblicati.

Come la CGUE ha sottolineato, «da un’interpretazione contestuale e sistematica dell’art. 12 della direttiva “vita privata e comunicazioni elettroniche” risulta che il consenso di cui al n. 2 di tale articolo riguarda lo scopo della pubblicazione dei dati personali in un elenco pubblico e non già l’identità di uno specifico fornitore di elenchi»[361]. Inoltre, «è la pubblicazione in sé di dati personali in un elenco avente uno scopo particolare che può risultare pregiudizievole per un abbonato»[362] piuttosto che l’identità di chi ha fornito i dati.

La causa *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV c. Autoriteit Consument en Markt (AMC)*[363] riguardava la richiesta della società belga che fornisce servizi di consultazione ed elenchi abbonati alle imprese che attribuiscono numeri di telefono ad abbonati nei Paesi Bassi, di ottenere l'accesso ai dati relativi ai loro abbonati. La società belga aveva invocato un obbligo previsto dalla direttiva servizio universale[364]. Tale obbligo impone alle aziende che attribuiscono numeri di telefono di mettere a disposizione tali numeri telefonici qualora ne venga fatta richiesta per la pubblicazione in elenchi, se gli abbonati hanno acconsentito alla pubblicazione dei propri numeri. Le società dei Paesi Bassi avevano rifiutato di farlo, affermando di non essere tenute a fornire i dati in questione a un'impresa stabilita in un altro Stato membro. Esse sostenevano che gli utenti avevano prestato il loro consenso alla pubblicazione dei propri numeri, restando inteso che sarebbero stati pubblicati in un elenco olandese. La CGUE ha sostenuto che la direttiva servizio universale include tutte le richieste da parte di fornitori di servizi elenco abbonati, indipendentemente dallo Stato membro in cui essi sono stabiliti. La CGUE ha inoltre stabilito che la trasmissione degli stessi dati a un'altra impresa che intende pubblicare un elenco pubblico senza ottenere nuovamente il consenso degli abbonati, non può ledere la sostanza stessa del diritto alla tutela dei dati personali[365]. Di conseguenza, non occorre che l'impresa che attribuisce i numeri di

telefono ai suoi abbonati formuli la richiesta di consenso dell'abbonato in maniera tale che quest'ultimo esprima il proprio consenso in modo distinto a seconda dello Stato membro verso il quale i dati che lo riguardano possono essere trasmessi[366].

Consenso inequivocabile

Ogni consenso deve essere manifestato in maniera inequivocabile[367]. Ciò sig- nifica che non dovrebbero sussistere dubbi ragionevoli in merito al fatto che

l'interessato volesse esprimere il proprio consenso al trattamento dei propri dati. Per esempio, l'inerzia di un interessato non indica un consenso inequivocabile.

Sarebbe questo il caso del titolare del trattamento che ottiene il consenso mediante dichiarazioni nella sua politica sulla vita privata, ad esempio «utilizzando il nostro servizio, acconsenti al trattamento dei tuoi dati personali». In questo caso, i titolari del trattamento potrebbero dover assicurare che gli utenti acconsentano manualmente e singolarmente a tali politiche.

Se il consenso viene prestato in forma scritta nell'ambito di un contratto, il con- senso per il trattamento dei dati personali deve essere individualizzato e in ogni caso dovrebbero esistere «garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene»[368].

Requisiti relativi al consenso dei minori

Il RGPD prevede una protezione specifica per i minori in relazione ai servizi della società dell'informazione, in quanto «possono essere meno consape- voli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali»[369]. Per- tanto, ai sensi del diritto dell'UE, quando i fornitori di ser vizi della società

dell'informazione trattano dati personali di minori di età inferiore a 16 anni sulla base del consenso, il trattamento sarà lecito «soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale»[370]. Gli Stati membri possono stabilire un'età inferiore nel diritto nazionale, purché non inferiore ai 13 anni[371]. Il consenso del titolare della responsabilità genitoriale non è necessario «nel quadro dei servizi di prevenzi- one o di consulenza forniti direttamente a un minore»[372]. Qualsiasi informazi- one e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente[373].

Il diritto di revoca del consenso in qualsiasi momento

Il RGPD include un diritto generale di revoca del consenso in qualsiasi momento[374]. L'interessato deve essere informato di tale diritto prima di pres- tare il proprio consenso e può esercitarlo a sua discrezione. Non ci dovrebbe essere alcun obbligo di motivazione per detta revoca e nessun rischio di con- seguenze negative al di là della cessazione di eventuali benefici derivanti dall'uso dei dati precedentemente concordato. Il consenso dovrebbe essere revocato con la stessa facilità con cui è accordato[375]. Non può esservi libero consenso se l'interessato non è in grado di revocare il proprio consenso senza subire pregiudizio, o se il consenso non può essere revocato con la stessa facil- ità con cui è stato accordato[376].

Esempio: un cliente accetta di ricevere corrispondenza promozionale a un indirizzo che fornisce a un titolare del trattamento. Se il cliente revoca il consenso, il titolare del trattamento deve interrompere immediatamente l'invio della corrispondenza promozionale. Non dovrebbero essere imposte conseguenze di natura pecuniaria a fini di ritorsione. La revoca, tuttavia, è esercitata per il futuro e non ha effetto retroattivo. Il periodo durante il quale i dati personali del cliente sono stati trattati in modo lecito, grazie al consenso del cliente, era legittimo. La revoca impedisce

l’ulteriore trattamento di tali dati, a meno che quest’ultimo sia svolto nel rispetto del diritto alla cancellazione[377].

Necessità di esecuzione di un contratto

Nell’ambito del diritto dell’UE, l’articolo 6, paragrafo 1, lettera b), del RGPD fornisce un’ulteriore base per la liceità del trattamento dei dati personali, e precisamente, che sia «necessario all’esecuzione di un contratto di cui l’interessato è parte». Tale disposizione comprende anche i rapporti precontrattuali. Ad esempio, nei casi in cui una parte intende stipulare un contratto,

ma non vi ha ancora provveduto, probabilmente perché restano da compiere alcuni controlli. Se una parte deve trattare i dati a tal fine, questo trattamento è legittimo fintantoché sia «necessario [...] all'esecuzione di misure precontrat- tuali adottate su richiesta dello stesso»[378].

La nozione di trattamento come «fondamento legittimo previsto dalla legge» di cui all'articolo 5, paragrafo 2, della Convenzione n. 108 modernizzata, com- prende anche il «trattamento dei dati necessari per l'esecuzione di un con- tratto (o di misure precontrattuali, adottate su richiesta dell'interessato) di cui l'interessato è parte»[379].

Obblighi legali del titolare del trattamento

Il diritto dell'UE prevede un altro motivo che rende legittimo il trattamento dei dati, ossia se «è necessario per adempiere un obbligo legale al quale è sog- getto il titolare del trattamento» (articolo 6, paragrafo 1, lettera c), del RGPD. Questa disposizione si riferisce ai titolari del trattamento che operano sia nel settore privato che nel pubblico; anche gli obblighi legali dei titolari del trat- tamento dei dati del settore pubblico possono rientrare nell'ambito di appli- cazione dell'articolo 6, paragrafo 1, lettera e), del RGPD. Vi sono molti esempi di situazioni in cui la legge obbliga i titolari del trattamento del settore privato a trattare dati riguardanti interessati specifici. Ad esempio, i datori

di lavoro devono trattare i dati dei propri dipendenti per motivi di previdenza sociale e fiscalità, e le aziende devono trattare i dati dei propri clienti per motivi di ordine fiscale.

L'obbligo legale può trovare la sua origine nel diritto dell'Unione o dello Stato membro, che potrebbe essere la base per una o più operazioni di trat ta- mento. Dovrebbe spettare a un atto legislativo stabilire la finalità del trat- tamento, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati, le limitazioni della finalità, il periodo di

conservazione e altre misure per garantire un trattamento lecito e corretto[380]. Qualsiasi legge di questo tipo che sia alla base del trattamento dei dati per- sonali deve essere conforme sia agli articoli 7 e 8 della Carta sia all'articolo 8 della CEDU.

Gli obblighi legali del titolare del trattamento costituiscono altresì la base per la legittimità del trattamento dei dati nell'ambito del diritto del CdE[381]. Come sot- tolineato in precedenza, gli obblighi giuridici di un responsabile del trattamento del settore privato sono solo uno dei casi specifici dei legittimi interessi altrui, come indicato all'articolo 8, paragrafo 2, della CEDU. Pertanto, l'esempio dei datori di lavoro che trattano i dati dei propri dipendenti è pertinente anche per il diritto del CdE.

Interessi vitali dell'interessato o di un'altra persona fisica

Nell'ambito del diritto dell'UE, l'articolo 6, paragrafo 1, lettera d), del RGPD, dispone che il trattamento di dati personali è lecito se «è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica». Il motivo legittimo può essere invocato solo per il trattamento di dati per- sonali fondato sull'interesse vitale di un'altra persona fisica quando tale trattamento «non può essere manifestamente fondato su un'altra base giuridica»[382]. A volte un tipo di trattamento può essere fondato sia su motivi di interesse

pubblico sia sugli interessi vitali dell'interessato o di un'altra per- sona. È questo il caso, per esempio, quando è necessario tenere sotto con- trollo l'evoluzione delle epidemie e la loro diffusione oppure in casi di emer- genze umanitarie.

Nel quadro del diritto del CdE, gli interessi vitali dell'interessato non sono men- zionati nell'articolo 8 della CEDU. Tuttavia, gli interessi vitali dell'interessato sono considerati impliciti nella nozione di «fondamento legit timo» di cui

all’articolo 5, paragrafo 2, della Convenzione n. 108 modernizzata, che tratta della legittimità del trattamento dei dati personali[383].

Interesse pubblico ed esercizio di pubblici poteri

Considerate le molteplici modalità con cui si possono organizzare le questioni pubbliche, l’articolo 6, paragrafo 1, lettera e), del RGPD, stabilisce che i dati personali possono essere trattati lecitamente se «è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento [...]»[384].

Esempio: nella causa *Huber c. Bundesrepublik Deutschland*[385], il sig. Huber, cittadino austriaco residente in Germania, ha chiesto all’Ufficio federale per l’immigrazione e i rifugiati di cancellare i dati che lo riguardano dal registro centrale degli stranieri (denominato «AZR»). Tale registro, contenente i dati personali relativi ai cittadini dell’UE che non hanno la cittadinanza tedesca e che risiedono in Germania da oltre tre mesi, è utilizzato per finalità statistiche nonché dalle forze dell’ordine e dalle autorità giudiziarie nell’ambito d’indagini e operazioni relative ad attività criminali o pregiudizievoli per la pubblica sicurezza. Il giudice del rinvio ha chiesto se il trattamento dei dati personali intrapreso nell’ambito di un registro come il registro centrale

degli stranieri, a cui anche altre autorità pubbliche hanno accesso, fosse compatibile con il diritto dell'UE, dal momento che non esiste un registro simile per i cittadini tedeschi.

La CGUE ha ritenuto che, ai sensi dell'articolo 7, lettera e), della direttiva 95/46[386], i dati personali possano essere trattati lecitamente se è necessario per l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri.

Secondo la CGUE, «considerato l'obiettivo di garantire un livello di tutela equivalente in tutti gli Stati membri, la nozione di necessità come risultante dall'art. 7, lett. e), della direttiva 95/46[387] [...] non può avere un contenuto variabile in funzione degli Stati membri. Si tratta quindi di una nozione autonoma del diritto comunitario che deve essere interpretata in maniera tale da rispondere pienamente alla finalità di tale direttiva come definita dal suo art. 1, n. 1»[388].

La Corte ha rilevato che il diritto alla libera circolazione di un cittadino dell'Unione nel territorio di uno Stato membro di cui questi non ha la nazionalità non è incondizionato e può essere subordinato alle limitazioni e alle condizioni previste dal trattato che istituisce la Comunità europea nonché dalle relative disposizioni di attuazione. Pertanto se, in linea di principio, è legittimo che uno Stato membro disponga di un registro centralizzato come l'AZR quale ausilio per le autorità incaricate di applicare la normativa in materia di soggiorno, un siffatto registro non può contenere informazioni diverse da quelle a tal fine necessarie. La CGUE ha concluso che un siffatto sistema per il trattamento dei dati personali è conforme al diritto dell'Unione se contiene unicamente i dati necessari per l'applicazione di detta normativa e se il suo carattere centralizzato consente un'applicazione più efficace di tale

normativa. Il giudice nazionale deve accertare se dette condizioni siano soddisfatte in questo caso particolare. Diversamente, la conservazione e il trattamento dei dati personali in un registro come l'AZR per finalità statistiche non possono, su qualsiasi base, essere considerati necessari ai sensi dell'articolo 7, lettera e)[389] della direttiva 95/46[390].

Infine, per quanto riguarda la questione dell'utilizzo dei dati contenuti nel registro per finalità di lotta alla criminalità, la CGUE ha ritenuto che questo obiettivo riguardi «necessariamente la repressione dei reati commessi, a prescindere dalla cittadinanza dei loro autori». Il registro in questione non contiene dati personali relativi ai cittadini dello Stato membro interessato e questa differenza di trattamento costituisce una discriminazione vietata dall'articolo 18 del TFUE. Di conseguenza, la CGUE ha stabilito che questa

disposizione «osta all'istituzione da parte di uno Stato membro, per finalità di lotta alla criminalità, di un sistema di trattamento di dati personali riguardante specificamente i cittadini dell'Unione non aventi la nazionalità di tale Stato membro»[391].

Anche l'utilizzo dei dati personali da parte delle autorità che operano nell'ambito pubblico è subordinato all'articolo 8 della CEDU ed è disciplinato, ove appropriato, dall'articolo 5 (2) della Convenzione n. 108 modernizzata.[392]

Interessi legittimi perseguiti dal titolare del trattamento o da terzi

Nell'ambito del diritto dell'UE, l'interessato non è l'unico soggetto portatore di interessi legittimi. [...] L'articolo 6, paragrafo 1, lettera f), del RGPD, stabilisce che i dati personali possono essere trattati in modo lecito se ciò «è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi [ad eccezione delle autorità pubbliche nell'esercizio dei loro compiti] cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela [...]»[393].

L'esistenza di un interesse legittimo deve essere attentamente valutata in ciascun caso

specifico[394]. Se l'interesse legittimo del titolare del trattamento viene individuato, deve essere effettuato un test comparativo tra tali interessi e gli interessi o i diritti e le libertà fondamentali della persona interessata[395]. In occasione di tale valutazione si devono tenere in considerazione le ragionevoli aspettative dell'interessato, per accertare se gli interessi del titolare del trattamento prevalgono sugli interessi o i diritti fondamentali dell'interessato[396]. Se i diritti dell'interessato prevalgono sugli interessi legittimi del titolare del trat- tamento, quest'ultimo può adottare misure e mettere in atto garanzie per

assicurare che l'impatto sui diritti dell'interessato sia ridotto al minimo (ad esempio, pseudonimizzando i dati), e invertire l'«equilibrio» prima di poter invocare in modo lecito questo fondamento legittimo per il trattamento. Nel suo parere sulla nozione di interessi legittimi del titolare del trattamento, il Gruppo di lavoro articolo 29 ha sottolineato il ruolo fondamentale della respon- sabilità e della trasparenza, nonché dei diritti dell'interessato di opporsi al trat- tamento dei propri dati, o al loro accesso, modifica, cancellazione o trasferi- mento, nell'equilibrare gli interessi legittimi del titolare del trattamento e gli interessi dei diritti fondamentali dell'interessato[397].

Nei considerando del RGPD vengono forniti alcuni esempi di ciò che costituisce un interesse legittimo del titolare del trattamento in questione. Per esempio, il trattamento di dati personali è consentito senza il consenso dell'interessato quando è effettuato per finalità di marketing diretto o quando si tratta del trat- tamento di dati «strettamente necessari a fini di prevenzione delle frodi»[398].

Nella sua giurisprudenza, la CGUE ha ampliato il criterio per determinare ciò che costituisce un interesse legittimo.

Esempio: la causa *Valsts Policijas Rīgas Regiona pārvaldes Kārtības Policijas pārvalde*[399] riguardava danni causati a un filobus della società di trasporti Rīgas dall'improvvisa apertura di una portiera di un taxi da parte di un passeggero. La Rīgas satiksme voleva agire nei confronti del passeggero per ottenere il risarcimento dei danni. Tuttavia, la polizia aveva comunicato solo il nome del passeggero, rifiutando di comunicare il numero del documento di identità e il domicilio e sostenendo che la comunicazione sarebbe stata illegale ai sensi delle leggi nazionali in materia di vita privata.

Il giudice del rinvio lettone ha chiesto alla CGUE di pronunciarsi in via pregiudiziale sulla questione di sapere se la legislazione dell'UE in materia di protezione dei dati imponga l'obbligo di comunicare tutti i dati personali

necessari per agire giudizialmente in sede civile nei confronti di una persona ritenuta responsabile di un'infrazione amministrativa[400].

La CGUE ha precisato che la normativa europea in materia di protezione dei dati prevede la possibilità – non un obbligo – di comunicare a un terzo i dati necessari a perseguire i suoi interessi legittimi[401]. La CGUE ha stabilito tre condizioni cumulative che devono essere soddisfatte affinché il trattamento dei dati personali sia lecito sulla base del motivo del «legittimo interesse»[402]. In primo luogo, il terzo a cui vengono comunicati i dati deve perseguire un interesse legittimo. Nella fattispecie, questo significa che chiedere informazioni personali al fine di agire in giudizio nei confronti di una persona per avere causato danni alla proprietà costituisce un legittimo interesse di terzi. In secondo luogo, il trattamento dei dati personali deve essere necessario per il perseguimento dell'interesse legittimo. In questo caso, ottenere informazioni personali quali l'indirizzo e/o il numero del documento di identità è strettamente necessario per stabilire l'identità di tale persona. In terzo luogo, i diritti e le libertà fondamentali dell'interessato non devono prevalere sugli interessi legittimi del titolare del trattamento o del terzo. La ponderazione degli interessi deve essere fatta caso per caso, tenendo conto di fattori quali la gravità della violazione dei diritti dell'interessato o addirittura, in determinate circostanze, l'età della persona. Nel caso specifico,

tuttavia, la CGUE non ha ritenuto giustificato il rifiuto della comunicazione per il solo fatto che l'interessato era minorenne.

Nella sentenza *ASNEF e FECEMD*, la CGUE si è pronunciata esplicitamente sul trattamento dei dati sulla base del motivo legittimo del «legittimo interesse», all'epoca sancito dall'articolo 7, lettera f), della direttiva sulla tutela dei dati[403].

Esempio: nella causa *ASNEF e FECEMD*[404], la CGUE ha chiarito che la normativa nazionale non è autorizzata ad aggiungere condizioni a quelle previste nell'articolo 7, lettera f), della direttiva per il trattamento lecito dei dati[405]. Questa precisazione fa riferimento a una situazione in cui il diritto spagnolo in materia di protezione dei dati conteneva una disposizione secondo la quale altre parti private potrebbero rivendicare un interesse legittimo nel trattamento dei dati personali solo se le informazioni fossero già apparse in fonti accessibili al pubblico.

La CGUE ha anzitutto rilevato che la direttiva 95/46/CE[406] mira a garantire che il livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento dei dati personali è equivalente in tutti gli Stati membri. Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nell'UE[407]. Di conseguenza, la CGUE ha dichiarato che «dall'obiettivo consistente nel garantire un livello di protezione equivalente in tutti gli Stati membri deriva che l'art. 7 della direttiva 95/46[408] prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito». Inoltre,

«gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali all'art. 7 di detta direttiva[409], né prevedere requisiti supplementari che vengano a modificare la portata di uno dei sei principi previsti da detto articolo»[410]. La CGUE ha ammesso che, per quanto riguarda la ponderazione necessaria in forza dell'articolo 7, lettera f), della direttiva 95/46/CE è possibile prendere in considerazione che la gravità della violazione dei diritti fondamentali della persona interessata da tale trattamento possa variare in funzione della circostanza che i dati di cui trattasi figurino già, o no, in fonti accessibili al pubblico.

Tuttavia, l’articolo 7, lettera f), della direttiva «osta a che uno Stato membro escluda in modo categorico e generalizzato la possibilità che talune categorie di dati personali siano oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco nel caso specifico».

Alla luce di tali considerazioni, la CGUE ha concluso che l’articolo 7, lettera f), della direttiva 95/46[411] deve essere interpretato nel senso che «osta ad una normativa nazionale che, in assenza del consenso della persona interessata e per autorizzare il trattamento dei suoi dati personali, necessario alla realizzazione del legittimo interesse perseguito dal responsabile di tale trattamento oppure dal o dai terzi ai quali tali dati vengono comunicati, richiede, oltre al rispetto dei diritti e delle libertà fondamentali di detta persona, che i dati in parola figurino in fonti accessibili al pubblico, escludendo quindi in modo categorico e generalizzato qualsiasi trattamento di dati che non figurino in tali fonti»[412].

Qualora i dati personali siano trattati basandosi sul motivo del «legit- timo interesse», l’interessato ha il diritto di opporsi in qualsiasi momento a tale trattamento per motivi connessi alla sua situazione particolare, ai sensi dell’articolo 21, paragrafo 1, del RGPD. Il titolare del trattamento deve astenersi dal trattare ulteriormente i dati, salvo

che dimostri l'esistenza di motivi legit- timi cogenti per continuare il trattamento.

Per quanto riguarda il diritto del CdE, formulazioni analoghe possono essere rinv- enute ed è disciplinato, ove appropriato, dall'articolo 5 (2) della Convenzione n.
108 modernizzata e nelle raccomandazioni del CdE. La raccomandazione sulla profilazione riconosce la legittimità del trattamento di dati personali per final- ità di profilazione se necessario per gli interessi legittimi altrui, «tranne qualora prevalgano su tali interessi i diritti e le libertà fondamentali degli interessati»[413]. Inoltre «la protezione dei diritti e delle libertà altrui» è menzionata nell'articolo 8, paragrafo 2, della CEDU come uno dei motivi legittimi per limitare il diritto alla protezione dei dati.

Esempio: nella causa *Y c. Turchia*,[414] il ricorrente era HIV positivo. Poiché durante il suo traspor to in ospedale era incosciente, l'equipaggi o dell'ambulanza aveva informato il personale dell'ospedale che egli era HIV positivo. Il ricorrente aveva sostenuto dinanzi alla Corte EDU che la divulgazione di tali informazioni aveva violato il suo diritto al rispetto della vita privata. Tuttavia, data la necessità di proteggere la sicurezza del personale ospedaliero, la condivisione delle informazioni non è stata considerata una violazione dei suoi diritti.

4.1.2. Il trattamento di categorie particolari di dati personali (dati sensibili)

Il diritto del CdE affida al diritto nazionale il compito di definire una protezi- one adeguata per l'utilizzo di dati sensibili, purché siano soddisfatte le con- dizioni dell'articolo 6 della Convenzione n. 108 modernizzata, ad esempio che adeguate garanzie a complemento delle ulteriori disposizioni della Conven- zione siano sancite dalla legge. Il diritto dell'UE, all'articolo 9 del RGPD, con- tiene un regime dettagliato per il trattamento di categorie particolari di dati (anche detti «dati sensibili»), che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale, non- ché per il trattamento di dati genetici e dati biometrici intesi a identificare in

modo univoco una persona fisica, e dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. In linea di principio il trattamento dei dati sensibili è vietato[415].

Esiste tuttavia un elenco esaustivo di deroghe a tale divieto, che figurano all'articolo 9, paragrafo 2, del regolamento e che costituiscono motivi legittimi per il trattamento di dati sensibili. Tali deroghe comprendono situazioni in cui:

- l'interessato acconsente esplicitamente al trattamento dei dati;

- il trattamento è effettuato da un organismo che non persegue scopi di lucro e riveste carattere politico, filosofico, religioso o sindacale nel corso di attività legittime e riguarda solo i suoi (ex) membri o persone che hanno contatti regolari con esso per tali scopi;

- il trattamento riguarda dati personali esplicitamente resi pubblici dall’interessato;

- il trattamento è necessario:

- per adempiere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell’interessato nel contesto dell’occupazione, della sicurezza sociale e della protezione sociale;

- per tutelare gli interessi vitali dell’interessato o di un’altra persona fisica
(quando l’interessato non può prestare il proprio consenso);

- per rivendicare, esercitare o difendere un diritto per via giudiziaria o quando i tribunali esercitano le loro funzioni giurisdizionali;

- per finalità di medicina preventiva o di medicina del lavoro: per la «val- utazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell’Unione o degli Stati membri o conforme- mente al contratto con un professionista della sanità»;

- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o stor- ica o a fini statistici;

- per motivi di interesse pubblico nel settore della sanità pubblica; o

- per motivi di interesse pubblico rilevante.

Per trattare categorie particolari di dati, un rapporto contrattuale con l'interessato non è quindi visto come fondamento giuridico per il trattamento legittimo di dati sensibili, ad eccezione di un contratto con un professionista della sanità vincolato dal segreto professionale[416].

Consenso esplicito dell'interessato

Nell'ambito del diritto dell'UE, la prima condizione possibile perché sia lecito il trattamento dei dati, a prescindere che siano sensibili o non sensibili, è il consenso dell'interessato. Nel caso di dati sensibili, tale consenso deve essere esplicito. Il diritto dell'Unione o dello Stato membro, tuttavia, può disporre che

il divieto di trattamento per le categorie particolari non possa essere revocato dall'interessato[417]. Potrebbe essere il caso, ad esempio, del trattamento che implica rischi inconsueti per l'interessato.

Diritto del lavoro o diritto della sicurezza e della protezione sociale

Ai sensi del diritto dell'Unione, il divieto di cui all'articolo 9, paragrafo 1, può essere revocato se il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti del titolare del trattamento o dell'interessato in mate- ria di lavoro o sicurezza sociale. Tuttavia, il trattamento deve essere autoriz- zato dal diritto dell'UE, dal diritto nazionale o da un contratto collettivo ai sensi del diritto nazionale, in presenza di garanzie appropriate per i diritti e gli interessi fondamentali dell'interessato[418]. I registri del personale tenuti da un'organizzazione posso no contenere dati perso nali sensi bili in pre- senza di talune condizioni specificate nel RGPD e nel pertinente diritto nazi- onale. Esempi di dati sensibili possono includere l'appartenenza a sindacati o informazioni riguardanti la salute.

Interessi vitali dell'interessato o di un'altra persona

Nell'ambito del diritto dell'UE, come nel caso dei dati non sensibili, i dati sen- sibili possono essere trattati

in ragione degli interessi vitali dell'interessato o di un'altra persona fisica[419]. Se il trattamento si fonda sull'interesse vitale di un'altra persona, tale motivo legittimo può essere invocato unicamente se tale trattamento «non può essere manifestamente fondato su un'altra base giuridica»[420]. In alcuni casi, il trattamento dei dati personali può proteggere sia gli interessi pubblici sia gli interessi privati; ad esempio, quando il trattamento è necessario a fini umanitari[421].

Affinché il trattamento dei dati sensibili sia legittimo su questa base, dovrebbe essere impossibile chiedere il consenso all'interessato in quanto, ad esempio, lo stesso era incosciente o assente e non poteva essere contattato. In altre

parole, la persona deve essere nell'incapacità fisica o giuridica di prestare il proprio consenso.

Enti di beneficenza o organismi senza scopo di lucro

Il trattamento dei dati personali è consentito anche nell'ambito delle legittime attività di fondazioni, associazioni o altri organismi senza scopo di lucro che perseguano finalità politiche, filosofiche, religiose o sindacali. Tuttavia, il tratta- mento deve riguardare unicamente i membri, gli ex membri o coloro che hanno regolari contatti con l'organismo[422]. I dati sensibili non possono essere comuni- cati all'esterno di tali organismi senza il consenso dell'interessato.

Dati resi manifestamente pubblici dall'interessato

L'articolo 9, paragrafo 2, lettera e), del RGPD stabilisce che il trattamento non è proibito se si riferisce a dati resi manifestamente pubblici dall'interessato. Anche se il significato di «resi manifestamente pubblici dall'interessato» non è definito nel regolamento, poiché si tratta di un'eccezione al divieto di tratta- mento dei dati sensibili, l'espressione deve essere interpretata restrittivamente e nel senso che richiede che l'interessato renda pubblici i propri dati personali deliberatamente. Pertanto, se la televisione trasmette un video tratto da una telecamera di sorveglianza, che mostra, tra l'altro, un vigile del

fuoco coinvolto in un incidente, nell'atto di evacuare un edificio, non si può ritenere che il vigile del fuoco abbia manifestamente reso pubblici i dati. D'altra parte, se il pomp- iere decide di descrivere l'incidente e pubblicare il video e le foto su una pagina Internet pubblica, si tratterebbe di un atto deliberato e positivo volto a rendere i dati pubblici. È importante notare che rendere pubblici i propri dati non costi- tuisce consenso, ma si tratta di un altro permesso per il trattamento di catego- rie particolari di dati.

Il fatto che l'interessato abbia reso pubblici i dati personali trattati non esenta i titolari del trattamento dai loro obblighi derivanti dal diritto in materia di pro- tezione dei dati. Ad esempio, il principio di limitazione della finalità continua ad applicarsi ai dati personali, anche se tali dati sono stati resi pubblici[423].

Azioni legali

Anche il trattamento di categorie particolari di dati «necessario per accertare, esercitare o difendere un diritto in sede giudiziaria», che sia in sede giudiziale, amministrativa o stragiudiziale[424], è consentito ai sensi del RGPD[425]. In questo caso, il trattamento deve essere rilevante per un'azione legale specifica e il suo esercizio o la sua difesa, rispettivamente, e può essere richiesto da una qual- siasi delle parti in causa.

Quando esercitano le loro funzioni giurisdizionali, i tribunali possono trattare categorie particolari di dati nell'ambito della risoluzione di una controversia legale[426]. Esempi di queste categorie particolari di dati, trattati in questo con- testo, potrebbero includere, ad esempio, i dati genetici nell'accertamento della filiazione o lo stato di salute quando una parte delle prove riguarda i dettagli di un danno subito da una vittima di reato.

Motivi di interesse pubblico rilevante

Ai sensi dell'articolo 9, paragrafo 2, lettera g), del RGPD, gli Stati membri pos- sono introdurre ulteriori circostanze in cui i dati sensibili possono essere trat- tati, purché:

- il trattamento dei dati avvenga per motivi di interesse pubblico rilevante;

- sia previsto dalla legislazione europea o nazionale;

- la legislazione europea o nazionale sia proporzionata, rispetti il diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti e gli interessi dell'interessato[427].

Un esempio significativo è costituito dai sistemi di cartelle cliniche elettroniche. Grazie a tali sistemi, i dati sanitari raccolti dagli operatori durante il trattamento di un paziente sono messi a disposizione di altri operatori sanitari che si occupano del paziente in questione su larga scala, di solito a livello nazionale.

Il Gruppo di lavoro articolo 29 ha concluso che l'istituzione di tali sistemi non potrebbe avvenire in base alle norme giuridiche vigenti che riguardano il tratta- mento dei dati sui pazienti[428]. I sistemi di cartelle cliniche elettroniche possono tuttavia esistere se si basano su «motivi di interesse pubblico rilevante»[429]. Ciò richiederebbe una base giuridica esplicita per la loro creazione, che conterrebbe inoltre le garanzie necessarie per una gestione sicura del sistema[430].

Altri presupposti per il trattamento di dati sensibili

Il RGPD prevede che i dati sensibili possono essere trattati quando il tratta- mento è necessario per[431]:

• finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;

• motivi di interesse pubblico nel settore della sanità pubblica, quali la pro- tezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto

dell’Unione o degli Stati membri. Il diritto deve prevedere misure appropriate e specifiche per tutelare i diritti dell’interessato;

- fini di archiviazione, di ricerca scientifica o storica o fini statistici sulla base del diritto dell’Unione o degli Stati membri. Il diritto deve essere proporzi- onato alla finalità perseguita, rispettare l’essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti e gli interessi dell’interessato.

Ulteriori condizioni previste dal diritto nazionale

Il RGPD consente inoltre agli Stati membri di introdurre o mantenere ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute[432].

4.2. Norme sulla sicurezza del trattamento

- Le norme sulla sicurezza del trattamento obbligano il titolare del trattamento e il responsabile del trattamento ad attuare misure tecniche e organizzative ade- guate per prevenire ogni ingerenza non autorizzata nelle operazioni di tratta- mento dei dati.

- Il livello necessario di sicurezza dei dati è determinato:

- dalle caratteristiche di sicurezza disponibili sul mercato per ogni tipo specifico di trattamento;

- dai costi;

- dai rischi del trattamento dei dati per i diritti e le libertà degli interessati.

- Garantire la riservatezza dei dati personali è parte di un principio generale ricon- osciuto nel regolamento generale sulla protezione dei dati.

Nell’ambito del diritto sia dell’UE sia del CdE, i titolari del trattamento hanno l’obbligo generale di essere trasparenti e responsabili nel trattamento dei dati personali, specie quando si tratta di violazioni dei dati personali. Nel caso di violazioni di dati personali, i titolari del trat tamento devono informare le autorità di controllo, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Anche gli interessati dovrebbero essere informati in merito alla violazione dei dati personali quando tale violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

4.2.1. Elementi di sicurezza dei dati

Conformemente alle disposizioni pertinenti contenute nel diritto dell’UE:

«Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio»[433].

Tali misure comprendono, tra l’altro:

- la pseudonimizzazione e la cifratura dei dati personali[434];

- la capacità di assicurare che i sistemi e i servizi di trattamento mantengano la riservatezza, l’integrità, la disponibilità e la resilienza[435];

- la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di perdita degli stessi[436].

- una procedura per testare, verificare e valutare l’efficacia delle misure al fine di garantire la sicurezza del trattamento[437].

Una disposizione analoga è prevista dal diritto del CdE:

«Ciascuna parte dispone che il titolare del trattamento e, se possibile, il responsabile del trattamento adottino le opportune misure di sicurezza contro eventuali rischi come l’accesso accidentale o non autorizzato,
la distruzione, la perdita, l’uso, la modifica o la divulgazione di dati personali»[438].

Ai sensi del diritto sia dell'UE sia del CdE, una violazione dei dati che potrebbe incidere sui diritti e sulle libertà degli individui obbliga il titolare del tratta- mento a notificare la violazione all'autorità di controllo (cfr. la sezione 4.2.3).

Spesso sono state elaborate anche norme industriali, nazionali e internazi- onali per il trattamento sicuro dei dati. Il marchio di certificazione europeo di tutela della privacy (EuroPriSe), per esempio, è un progetto eTEN (reti tran- seuropee nel settore delle telecomunicazioni) dell'UE che valuta le possibilità di certificare prodotti, in particolare software, per facilitare la conformità con il diritto europeo in materia di protezione dei dati. L'Agenzia dell'Unione euro- pea per la sicurezza delle reti e dell'informazione (ENISA) è stata istituita per accrescere la capacità dell'UE, dei suoi Stati membri e della comunità impren- ditoriale, di prevenire, affrontare e rispondere ai problemi di sicurezza infor- matica e di rete[439]. L'ENISA pubblica regolarmente analisi delle attuali minacce alla sicurezza nonché consigli su come affrontarle[440].

La sicurezza dei dati non si ottiene solo mettendo in atto gli strumenti giusti, quali hardware e software, ma richiede anche adeguate norme organizzative interne. Tali norme interne dovrebbero includere idealmente i seguenti aspetti:

- trasmissione periodica a tutto il personale delle informazioni riguardanti le norme sulla sicurezza dei dati e i loro obblighi ai sensi del diritto in mate- ria di protezione dei dati, specialmente per quanto riguarda gli obblighi di riservatezza;

- distribuzione chiara delle responsabilità e delineazione netta delle compe- tenze in tema di trattamento dei dati, specie in relazione alle decisioni di trattare i dati personali e di trasmetterli a terzi o agli interessati;

- utilizzo dei dati personali solo in osservanza delle istruzioni impartite dalla persona competente o secondo le norme generali vigenti;

- protezione dell'accesso alle sedi e all'hardware e al software del titolare del trattamento o del responsabile del trattamento, compresi i controlli relativi all'autorizzazione dell'accesso;

- garanzia che le autorizzazioni dell'accesso ai dati personali siano state asseg- nate dalla persona competente su richiesta della documentazione adeguata;

- protocolli automatizzati sull'accesso ai dati personali con mezzi elettronici e controlli regolari di tali protocolli da parte dell'ufficio di vigilanza interna (imponendo quindi la registrazione di tutte le attività di trattamento);

- accurata documentazione per altre forme di divulgazione oltre all'accesso automatizzato ai dati, al fine di dimostrare che non ha avuto luogo alcuna trasmissione illegale di dati.

L'offerta di un'adeguata formazione e istruzione sulla sicurezza dei dati a tutti i membri del personale costituisce ugualmente un elemento importante delle precauzioni effettive in materia di sicurezza. Inoltre, è necessario attuare pro- cedure di verifica intese a garantire che le misure adeguate non siano solt- anto teoriche ma vengano attuate e funzionino concretamente (come gli audit interni o esterni).

Le misure volte a migliorare il livello di sicurezza di un titolare del trattamento o di un responsabile del trattamento prevedono strumenti quali l'intervento di responsabili della protezione dei dati personali, la formazione del personale in tema di sicurezza, audit regolari, test d'intrusione e marchi di qualità.

Esempio: nella causa *I c. Finlandia*[441], la ricorrente non era stata in grado di dimostrare che altri dipendenti dell'ospedale per cui lavorava avevano avuto accesso alle sue cartelle cliniche sanitarie in modo illecito. La violazione del proprio diritto alla protezione dei dati, asserita dalla ricorrente, era stata pertanto respinta dai giudici nazionali. La Corte EDU ha concluso che vi era stata una violazione dell'articolo 8 della CEDU, poiché il sistema dei registri dell'ospedale per la gestione delle cartelle cliniche «non consentiva di chiarire retroattivamente quale uso fosse stato fatto dei registri dei pazienti, dal momento che recava solamente le ultime cinque consultazioni più recenti e che tali informazioni venivano cancellate dopo il ritorno delle cartelle negli

archivi». La Corte EDU ha ritenuto decisivo il fatto che il sistema dei registri in uso nell'ospedale fosse stato chiaramente in contrasto con gli obblighi legali previsti dalla normativa nazionale, aspetto che non aveva ricevuto la debita considerazione da parte dei giudici nazionali.

L'UE ha adottato la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)[442], che è il primo strumento giuridico a livello dell'UE in materia di sicurezza informatica. La direttiva mira, da un lato, a migliorare la sicurezza informatica a livello nazionale e, dall'altro, ad aumentare il livello della cooper- azione nell'ambito dell'UE. Inoltre, essa impone obblighi agli operatori di servizi essenziali (inclusi gli operatori nei settori dell'energia, sanitario, bancario, dei trasporti, delle infrastrutture digitali, ecc.) e ai fornitori di servizi digitali, per gestire i rischi, garantire la sicurezza della loro rete e dei loro sistemi informa- tivi e comunicare gli incidenti a carico della sicurezza.

Prospettiva

Nel set tembre 2017, la Commissione europea ha proposto un proget to di regolamento volto a riformare il mandato dell'ENISA, per tenere conto delle nuove competenze e responsabilità dell'agenzia ai sensi della direttiva NIS. L'obiettivo del progetto di regolamento è di sviluppare le

attività dell'ENISA e rafforzare il suo ruolo come il «punto di riferimento nell'ecosistema della cib- ersicurezza dell'UE»[443]. Il progetto di regolamento dovrebbe lasciare impregiu- dicati i principi del RGPD e, chiarendo gli elementi necessari che costituiscono i sistemi europei di certificazione della cibersicurezza, dovrebbe anche raf- forzare la sicurezza dei dati personali. Parallelamente, nel settembre 2017, la Commissione europea ha proposto un progetto di regolamento di esecuzione che specifica gli elementi di cui i fornitori di servizi digitali devono tener conto per garantire la sicurezza delle loro reti e dei loro sistemi di informazione, come richiesto dall'articolo 16, paragrafo 8, della direttiva NIS. Al momento della redazione di questo manuale, le discussioni su queste due proposte erano in corso.

4.2.2. Riservatezza

Ai sensi del diritto dell'UE, il RGPD riconosce la riservatezza dei dati personali come parte di un principio generale[444]. I fornitori di servizi di comunicazione elettronica accessibili al pubblico devono assicurare la riservatezza. Essi hanno altresì l'obbligo di salvaguardare la sicurezza dei servizi da essi offerti[445].

Esempio: una dipendente di una compagnia assicurativa riceve una telefonata sul luogo di lavoro da qualcuno che afferma di essere un cliente e richiede informazioni relative al proprio contratto assicurativo.

L'obbligo di mantenere i dati del cliente riservati esige che la dipendente applichi perlomeno misure di sicurezza minime prima di divulgare i dati personali. Ciò potrebbe essere fatto, per esempio, proponendo di richiamare al numero di telefono riportato nel fascicolo del cliente.

Ai sensi dell'articolo 5, paragrafo 1, lettera f), i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, com- presa la protezione, mediante misure tecniche e organiz zative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla

distruzione o dal danno accidentali («integrità e riservatezza»).

In forza dell’articolo 32, il titolare del trattamento e il responsabile del trat- tamento devono mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza elevato. Tali misure includono, tra l’altro, la pseudoni- mizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza del trat- tamento, la valutazione e la verifica dell’efficacia delle misure e la capacità di ripristinare il trattamento in caso di incidente fisico o tecnico. Inoltre, l’adesione a un codice di condotta approvato o a un meccanismo di certificazione appro- vato può essere utilizzata come elemento per dimostrare il rispetto del prin- cipio di integrità e riservatezza. Inoltre, ai sensi dell’articolo 28 del RGPD, il contratto che vincola il titolare del trattamento al responsabile del trattamento deve prevedere che quest’ultimo si assicuri che le persone autorizzate a trat- tare i dati personali si siano impegnate alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza.

L’obbligo di riservatezza non si estende alle situazioni in cui i dati sono portati a conoscenza di una persona in qualità di privato e non come dipendente di un titolare o di un responsabile del trattamento. In questo caso, gli articoli 32 e 28 del RGPD non si applicano poiché l’utilizzo dei dati personali da parte di privati esula completamente dall’ambito di applicazione del regolamento nei casi laddove tale utilizzo rientri nella cosiddetta esenzione per l’esercizio di attività a carattere personale o domestico[446]. Tale esenzione riguarda l’utilizzo dei dati personali «da una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico»[447]. In seguito alla sentenza della CGUE pronunciata nella causa *Bodil Lindqvist*[448], detta esenzione deve essere però interpretata in senso restrittivo, specialmente per quanto riguarda la divulgazi- one dei dati. In particolare, l’esenzione per l’esercizio di attività a carattere per- sonale o domestico non si estende alla pubblicazione di dati personali a uso di un numero illimitato di destinatari su Internet o al trattamento di dati che presenta aspetti professionali o commerciali (per maggiori dettagli sulla causa cfr. le sezioni 2.1.2, 2.2.2 e 2.3.1).

La «riservatezza delle comunicazioni» è un altro aspetto della riservatezza, che è soggetto a *lex specialis*. Le norme speciali per assicurare la riservatezza delle comunicazioni elettroniche ai sensi della direttiva e-privacy impongono agli Stati

membri di vietare l’ascolto, la captazione, la memorizzazione o altre forme di intercettazione o di sorveglianza delle comunicazioni e dei relativi metadati, ad opera di persone diverse dagli utenti, o senza il consenso di questi ultimi[449]. Il diritto nazionale può autorizzare eccezioni a tale principio solo a fini di salvaguardia della sicurezza nazionale, della difesa, della prevenzione o del perseguimento di reati, e solo se tali misure sono necessarie e proporzionate agli obiettivi perseguiti[450]. Le stesse norme si applicheranno nell’ambito del futuro regolamento e-privacy, ma il campo di applicazione dell’atto giuridico sulla e-privacy sarà esteso dai servizi di comunicazione elettronica accessi- bili al pubblico alle comunicazioni effettuate attraverso servizi «over-the-top» (come le applicazioni mobili).

In base al diritto del CdE, l'obbligo di riservatezza è implicito nella nozione di sicurezza dei dati di cui all'articolo 7, paragrafo 1, della Convenzione n. 108 modernizzata, vertente sulla sicurezza dei dati.

Per i responsabili del trattamento, riservatezza significa che, senza autorizzazi- one, non possono divulgare i dati a terzi o ad altri destinatari. Per i dipendenti di un titolare o di un responsabile del trattamento, la riser vatezza implica l'utilizzo dei dati personali solo attenendosi alle istruzioni dei propri superiori competenti.

L'obbligo di riservatezza deve essere incluso in qualsiasi contratto stipulato tra i titolari del trattamento e i relativi responsabili. Inoltre, i titolari e i responsa- bili del trattamento dovranno adottare misure specifiche per far sì che i propri dipendenti siano subordinati a un obbligo giuridico di riservatezza, general- mente definito mediante l'inclusione di clausole di riservatezza nel contratto di lavoro del dipendente.

La violazione dell'obbligo professionale di riservatezza è punibile ai sensi del diritto penale in molti Stati membri dell'UE e parti contraenti della Convenzione n. 108.

4.2.3. Notifica di violazioni dei dati personali

Per violazione di dati personali si intende una violazione della sicurezza che compor ta accidentalmente o in modo illecito la distruzione, la perdita, la modifica o la divulgazione non autorizzata o l'accesso a dati personali trat- tati[451]. Mentre le nuove tecnologie, come la crittografia, offrono oggi mag- giori possibilità di garantire la sicurezza del trattamento, le violazioni dei dati restano ancora un fenomeno comune. Le cause delle violazioni di dati possono andare da errori accidentali da parte di persone che lavorano all'interno di un'organizzazione a minacce esterne, come hacker e organizzazioni di crimi- nalità informatica.

Le violazioni dei dati possono recare grave pregiudizio alla vita privata e alla protezione dei dati delle persone che, a seguito della violazione, perdono il controllo sui loro dati personali. Le violazioni possono portare a furto o usur- pazione d'identità, perdite finanziarie o danni materiali, perdita di riservatezza dei dati personali protetti da segreto professionale e pregiudizio alla repu- tazione dell'interessato. Nelle sue linee guida sulla notifica delle violazioni di dati personali ai sensi del regolamento (UE) 2016/679, il Gruppo di lavoro arti- colo 29 spiega che le violazioni possono avere tre tipi di effetto sui dati per- sonali: divulgazione, perdita e/o modifica[452]. Oltre all'obbligo di adottare misure per garantire la sicurezza del trattamento, come illustrato nella sezione 4.2, è altrettanto importante garantire che, quando si verificano violazioni, i titolari del trattamento le affrontino in modo adeguato e tempestivo.

Le autorità di controllo e i singoli individui sono spesso inconsapevoli del veri- ficarsi di una violazione dei dati e ciò impedisce loro di adottare misure per proteggersi dalle conseguenze negative. Per affermare i diritti delle persone e limitare l'impatto delle violazioni dei dati personali, l'UE e il CdE impongono un obbligo di notifica ai titolari del trattamento in determinate circostanze.

Ai sensi della Convenzione n. 108 modernizzata del CdE, le parti contraenti devono, come minimo,

prevedere che i titolari del trattamento notifichino le autorità di controllo competenti in merito a violazioni di dati suscettibili di interferire gravemente con i diritti degli interessati. Tale notificazione dovrebbe essere effettuata «senza indugio»[453].

Il diritto dell'UE stabilisce un regime dettagliato che disciplina i tempi e i conte- nuti delle notifiche[454]. Di conseguenza, i titolari del trattamento dei dati devono notificare determinate violazioni dei dati alle autorità di controllo senza ingius- tificato ritardo e, se possibile, entro 72 ore dal momento in cui vengono a con- oscenza della violazione. Qualora sia superato il periodo di 72 ore, le notifiche devono essere corredate di una spiegazione del ritardo. I titolari del tratta- mento sono esenti dall'obbligo di notifica solo qualora siano in grado di dimos- trare che è improbabile che la violazione dei dati possa presentare un rischio per i diritti e le libertà degli interessati.

Il regolamento specifica le informazioni minime da includere nella notifica per consentire all'autorità di controllo di adot tare i prov vedimenti neces- sari[455]. La notifica deve includere, come minimo, una descrizione della natura della violazione dei dati, nonché delle categorie e del numero approssimativo di interessati, e una descrizione delle probabili conseguenze della violazione e delle misure adottate dal responsabile del trattamento per porvi rimedio e attenuarne le conseguenze. Inoltre, dovrebbero essere forniti il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di con- tatto, per consentire all'autorità di controllo competente di ottenere ulteriori informazioni, se necessario.

Quando una violazione dei dati personali è suscettibile di presentare rischi elevati per i diritti e le libertà delle persone, i titolari del trattamento devono comunicare la violazione a tali persone (gli interessati) senza ingiustificato ritardo[456]. Le comunicazioni agli interessati, compresa la descrizione della violazione dei dati, devono essere redatte con un linguaggio semplice e chi- aro e contenere informazioni analoghe a quelle richieste per le notifiche alle autorità di controllo. In alcune circostanze, i titolari del trattamento possono essere esenti dall'obbligo di notifica di tali violazioni agli interessati. Le esen- zioni si applicano quando il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali

misure erano state appli- cate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad acced- ervi, quali la cifratura. L’azione intrapresa dal titolare del trattamento dopo la violazione per scongiurare il sopraggiungere di danni per i diritti degli interes- sati può anch’essa esentare il titolare dall’obbligo di darne comunicazione agli interessati. Infine, se detta comunicazione comporta uno sforzo sproporzionato da parte del titolare del trattamento, gli interessati possono essere informati della violazione tramite altri mezzi, quali una comunicazione pubblica o misure simili[457].

L’obbligo di notificare le violazioni dei dati alle autorità di controllo e agli inter- essati è rivolto ai titolari del trattamento. Tuttavia, possono verificarsi violazi- oni dei dati indipendentemente dal fatto che il trattamento sia effettuato da un titolare del trattamento o da un responsabile del trattamento. Per questo

motivo, è fondamentale garantire che anche i responsabili del trattamento siano tenuti a segnalare le violazioni dei dati. In questo caso, i responsabili del trattamento devono informare il titolare del trattamento delle violazioni dei dati, senza ingiustificato ritardo[458]. Il titolare del trattamento è quindi respon- sabile della notifica alle autorità di controllo e agli interessati, nel rispetto delle regole e dei tempi di cui sopra.

4.3. Norme in materia di responsabilità e promozione del rispetto delle norme

- Per garantire la responsabilità nel trattamento dei dati personali, titolari del trat- tamento e responsabili del trattamento devono tenere un registro delle attività di trattamento effettuate sotto la loro responsabilità e, su richiesta, trasmetterlo alle autorità di controllo.

- Il regolamento generale sulla protezione dei dati prevede diversi strumenti per promuovere il rispetto delle norme:

- la nomina di responsabili della protezione dei dati in determinate situazioni;

- lo svolgimento di una valutazione d’impatto prima dell’inizio di attività di trattamento che potrebbero presentare rischi elevati per i diritti e le libertà delle persone;

- consultazione preventiva dell’autorità di controllo competente qualora la val- utazione d’impatto indichi che il trattamento presenta rischi elevati che non possono essere attenuati;

- codici di condotta per i titolari e i responsabili del trattamento, che precisino l’applicazione del regolamento in vari settori di trattamento;

- meccanismi di certificazione, sigilli e marchi.

- Nella Convenzione n. 108 modernizzata, il diritto del CdE propone strumenti simili per la promozione del rispetto delle norme.

Il principio di responsabilizzazione è particolarmente importante per garantire l’applicazione delle norme in materia di protezione dei dati in Europa. Il titolare

del trattamento è responsabile del rispetto delle norme sulla protezione dei dati e deve essere in grado di dimostrarlo. La responsabilità non dovrebbe essere chiamata in causa solo dopo che si è verificata una violazione. I titolari del trat- tamento hanno piuttosto l'obbligo proattivo di seguire politiche adeguate di ges- tione dei dati, in tutte le fasi del trattamento. La normativa europea in materia di protezione dei dati impone ai titolari del trattamento di attuare misure tecniche e organizzative per garantire ed essere in grado di dimostrare che il trattamento è effettuato nel rispetto della legge. Tra tali misure figurano la nomina di respon- sabili della protezione dei dati, la tenuta di registri e documentazione relativi al trattamento nonché lo svolgimento di valutazioni d'impatto sulla vita privata.

4.3.1. Responsabili della protezione dei dati

I responsabili della protezione dei dati (RPD) sono persone che forniscono consulenza sul rispetto delle norme in materia di protezione dei dati nelle organizzazioni che effettuano il trattamento dei dati. Essi costituiscono «car- dini della responsabilità», in quanto facilitano il rispetto delle norme, agendo al tempo stesso da intermediari tra le autorità di controllo, gli interessati e l'organizzazione da cui sono stati designati.

Nell’ambito del diritto del CdE, l’articolo 10, paragrafo 1, della Convenzione n. 108 modernizzata, attribuisce ai titolari e ai responsabili del trattamento una responsabilità generale. Ciò esige che i titolari e i responsabili del trattamento adottino tutte le misure appropriate per conformarsi alle norme in materia di protezione dei dati previste dalla Convenzione e siano in grado di dimostrare che il trattamento dei dati sotto il loro controllo è conforme alle disposizioni della Convenzione. Anche se la Convenzione non specifica le misure concrete che i titolari e i responsabili del trattamento dovrebbero adottare, la relazione esplicativa della Convenzione n. 108 modernizzata indica che la nomina di un RPD potrebbe essere una misura potenzialmente idonea a dimostrare il rispetto della Convenzione. Gli RPD dovrebbero disporre di tutti i mezzi necessari per l’adempimento del loro mandato[459].

Contrariamente al diritto del CdE, nell’UE la nomina di un responsabile della protezione dei dati non è sempre a discrezione dei titolari e dei responsabili del trattamento, ma è obbligatoria a determinate condizioni. Il RGPD riconosce al RDP un ruolo fondamentale nel nuovo sistema di governance e prevede

disposizioni dettagliate per quanto riguarda la sua nomina, la posizione, i com- piti e le funzioni[460].

Il RGPD rende obbligatoria la nomina di un RPD in tre casi specifici: se il tratta- mento è svolto da un'autorità pubblica o da un organismo pubblico; se le attiv- ità principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala oppure se le attività principali consistono nel trat- tamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati[461]. Anche se termini quali «monitoraggio sistema- tico su vasta scala» e «attività essenziali» non sono definiti nel regolamento, il Gruppo di lavoro articolo 29 ha pubblicato linee guida su come interpretarli[462].

Esempio: è probabile che le imprese di social media e i motori di ricerca siano considerati titolari del trattamento le cui operazioni di trattamento richiedono un monitoraggio regolare e sistematico su vasta scala degli interessati. Il modello aziendale di tali società si fonda sul trattamento di grandi quantità di dati personali, che generano ricavi significativi attraverso l'offerta di servizi di pubblicità mirata e la possibilità per le aziende di pubblicizzare sui siti. La pubblicità mirata è un modo di pubblicare annunci pubblicitari in base

all’andamento demografico e alla storia o al comportamento d’acquisto precedente dei consumatori. Essa richiede quindi il monitoraggio sistematico delle abitudini e dei comportamenti online degli interessati.

Esempio: un ospedale e una compagnia di assicurazione sanitaria sono esempi tipici di titolari del trattamento le cui attività consistono nel trattamento su larga scala di categorie particolari di dati personali. I dati che rivelano informazioni riguardanti la salute di una persona costituiscono categorie particolari di dati personali ai sensi del diritto sia dell’UE sia del CdE e meritano pertanto una maggiore protezione. Il diritto dell’UE riconosce inoltre i dati genetici e i dati biometrici come categorie particolari. Nella misura in cui strutture sanitarie e compagnie di assicurazione trattano tali dati su larga scala esse sono tenute, ai sensi del RGPD, a nominare un responsabile della protezione dei dati.

Inoltre, l'articolo 37, paragrafo 4, del RGPD, prevede che nei casi diversi dai tre obbligatori di cui all'articolo 37, paragrafo 1, il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresent- anti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono des- ignare un responsabile della protezione dei dati.

Tutte le altre organizzazioni non sono giuridicamente obbligate a designare un RPD. Nondimeno, il RGPD prevede che i titolari del trattamento e i responsabili del trattamento possano scegliere di designare volontariamente un RPD, pur lasciando agli Stati membri la possibilità di rendere tale designazione obbliga- toria per un numero maggiore di organizzazioni rispetto a quelle previste dal regolamento[463].

Una volta che abbia designato un RPD, un titolare del trattamento deve assi- curarsi che quest'ultimo «sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali» all'interno dell'organizzazione[464]. Ad esempio, gli RPD dovrebbero essere coinvolti nel fornire consulenza in merito allo svolgimento delle valutazioni d'impatto sulla protezione dei dati e nel creare e conservare registrazioni delle attività di trat- tamento in un'organizzazione. Per consentire ai RPD di svolgere efficacemente i loro compiti, i

titolari del trattamento e i responsabili del trattamento sono tenuti a fornire loro le risorse necessarie, comprese le risorse finanziarie, le infrastrutture e le attrezzature. Tra i requisiti supplementari figurano la conces- sione ai RPD di tempo sufficiente per svolgere le loro funzioni e una formazi- one permanente che consenta agli stessi di sviluppare le proprie competenze e rimanere aggiornati con tutti gli sviluppi in materia di protezione dei dati[465].

Il RGPD stabilisce alcune garanzie di base per assicurare che gli RPD agiscano in maniera indipendente. I titolari del trattamento e i responsabili del trattamento devono assicurare che nell'esecuzione dei propri compiti relativi alla protezione dei dati, gli RPD non ricevano alcuna istruzione dall'azienda, incluse le persone al vertice gerarchico. Inoltre, essi non possono essere rimossi o penalizzati in

alcun modo per l’adempimento dei propri compiti[466]. Si consideri, ad esempio, il caso in cui il RPD consiglia a un titolare o a un responsabile dei dati di effet- tuare una valutazione d’impatto sulla protezione dei dati perché ritiene che il trattamento possa comportare un rischio elevato per gli interessati. L’impresa non concorda con il parere del RPD, non lo ritiene fondato e decide pertanto di non procedere a una valutazione d’impatto. L’azienda può ignorare il parere, ma non può rimuovere o penalizzare il RPD per averlo fornito.

Infine, l’articolo 39 del RGPD specifica i compiti e le funzioni degli RPD. Questi includono gli obblighi di informare e fornire consulenza alle aziende, nonché ai dipendenti che seguono il trattamento, in merito ai loro obblighi derivanti dalla legislazione, sorvegliare l’osservanza delle norme dell’UE e nazionali sulla protezione dei dati attraverso attività di controllo e la formazione del personale che partecipa ai trattamenti. Gli RPD devono inoltre cooperare con l’autorità di controllo e fungere da punto di contatto per quest’ultima per questioni connesse al trattamento dei dati come, per esempio, una violazione dei dati personali.

Per quanto riguarda i dati personali gestiti dalle istituzioni e dagli organismi dell’UE, il regolamento n. 45/2001 prevede l’obbligo per ogni istituzione e organismo di nominare un RPD. Il RPD è incaricato di garantire che le dispo- sizioni del regolamento

siano applicate correttamente nell'ambito delle istituz- ioni e degli organismi dell'UE e che sia gli interessati sia i titolari del tratta- mento dei dati siano informati dei propri diritti e obblighi[467]. Essi sono altresì responsabili di rispondere alle richieste del GEPD e di cooperare con lo stesso ove necessario. In modo analogo al RGPD, il regolamento n. 45/2001 contiene disposizioni riguardanti l'indipendenza degli RPD nello svolgimento delle loro funzioni e la necessità di dotarli del personale e delle risorse necessarie[468]. Gli RPD devono essere informati prima che un'istituzione o un organismo dell'UE (o dipartimenti di tali organizzazioni) eseguano trattamenti di dati e devono tenere un registro di tutti i trattamenti notificati[469].

4.3.2. Registri delle attività di trattamento

Per essere in grado di dimostrare la conformità ed essere ritenute responsa- bili, le aziende hanno spesso l'obbligo giuridico di documentare e registrare le loro attività. Un esempio significativo è dato dalle leggi e dai controlli in mate- ria di imposte, che richiedono a tutte le aziende di tenere registri e un'ampia documentazione. È importante stabilire obblighi simili anche in altri settori del diritto, in particolare del diritto in materia di protezione dei dati, dal momento che la tenuta dei registri è un modo importante per agevolare il rispetto delle norme in materia di protezione dei dati. Il diritto dell'UE stabilisce, pertanto, che i titolari del trattamento, o i loro rappresentanti, devono tenere un regis- tro delle attività di trattamento svolte sotto la propria responsabilità[470]. Tale obbligo ha lo scopo di assicurare che, qualora sia necessario, le autorità di con- trollo dispongano della documentazione necessaria per consentire loro di con- fermare la liceità del trattamento.

Le informazioni da documentare comprendono:

- nome e dati di contatto del titolare del trattamento e del contitolare del trattamento, del rappresentante del titolare del trattamento e del RPD, ove applicabile;

- finalità del trattamento;

- descrizione delle categorie di interessati e delle categorie di dati personali connessi al trattamento;

- informazioni sulle categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

- informazioni che indichino se sono stati effettuati, o saranno effettuati, trasferimenti di dati personali verso paesi terzi o organizzazioni internazi- onali; o

- ove possibile, i termini previsti per la cancellazione delle diverse catego- rie di dati personali, nonché una descrizione generale delle misure tecniche adottate per garantire la sicurezza del trattamento[471].

L'obbligo di tenere un registro delle attività ai sensi del RGPD non riguarda solamente i titolari, ma anche i responsabili del trattamento dei dati. Si tratta di uno sviluppo importante dal momento che, prima dell'adozione del regola- mento, il contratto stipulato tra il titolare del trattamento e il responsabile del trattamento riguardava principalmente gli obblighi di quest'ultimo. Il loro obbligo di tenuta dei registri è ora direttamente previsto per legge.

Il RGPD prevede un'eccezione a tale obbligo. L'obbligo di tenere un registro non si applica a un'impresa o organizzazione (titolare o responsabile del trat- tamento) con meno di 250 dipendenti. Tale eccezione, tuttavia, è soggetta alle condizioni che l'organizzazione di cui trattasi non effettui un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati, che il trat- tamento sia solo occasionale e non includa le categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

La tenuta di registri delle attività di trattamento dovrebbe consentire a titolari del trattamento e a responsabili del trattamento di dimostrare la conformità al regolamento. Dovrebbe altresì consentire alle autorità di controllo di monit- orare la liceità del trattamento. Se un'autorità di controllo chiede l'accesso a tali registri, i titolari del

trattamento e i responsabili del trattamento sono tenuti a cooperare e a renderli disponibili.

4.3.3. Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Le operazioni di trattamento presentano alcuni rischi inerenti ai diritti delle persone. I dati personali possono essere persi, comunicati a parti non autorizzate o trattati in modo illegale. Naturalmente, i rischi variano a seconda della natura e della portata del trattamento. Le operazioni su larga scala che comportano il trattamento di dati sensibili, per esempio, presentano un livello di rischio molto più elevato per gli interessati, rispetto ai potenziali rischi quando una piccola impresa tratta gli indirizzi e i numeri di telefono personali dei propri dipendenti.

Con l'emergere di nuove tecnologie e l'accresciuta complessità del trattamento, i titolari del trattamento devono affrontare tali rischi analizzando il probabile impatto del trattamento previsto, prima dell'inizio di tale attività. Ciò consente

alle organizzazioni di identificare, affrontare e mitigare adeguatamente i rischi con anticipo, limitando significativamente la probabilità di un impatto negativo sulle persone in conseguenza del trattamento.

Valutazioni d'impatto sulla protezione dei dati sono previste nell'ambito del diritto sia dell'UE sia del CdE. Nel quadro giuridico del CdE, l'articolo 10 para- grafo 2 della Convenzione n. 108 modernizzata, impone alle parti contraenti di assicurare che i titolari e i responsabili del trattamento «procedano, prima dell'inizio del trattamento previsto, all'esame dell'impatto potenziale dello stesso sui diritti e sulle libertà fondamentali degli interessati» e, a seguito della valutazione, concepiscano il trattamento dei dati in modo da prevenire o mini- mizzare i rischi legati allo stesso.

Il diritto dell'UE impone un obbligo analogo, più dettagliato, ai titolari del trat- tamento che rientrano nell'ambito di applicazione del RGPD. L'articolo 35 stabi- lisce che, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone, deve essere effettuata una valutazione d'impatto. Il regolamento non definisce come valutare la probabilità del rischio ma indica, piuttosto, quali potrebbero essere tali rischi[472]. Esso contiene un elenco dei trattamenti considerati a rischio elevato e per i quali è particolarmente

neces- saria una valutazione preliminare dell'impatto, e precisamente quando:

- i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche (profilazione);

- vengono trattati su larga sala dati sensibili o dati personali relativi a con- danne penali e reati;

- il trattamento richiede una sorveglianza sistematica su larga scala di zone accessibili al pubblico.

Le autorità di controllo devono adottare e rendere pubblico un elenco delle tipologie di trat tamento soggette a una valutazione d'impatto. Esse pos- sono inoltre redigere un elenco delle operazioni di trattamento esenti da tale obbligo[473].

Quando la valutazione d’impatto è necessaria, i titolari del trattamento devono valutare la necessità e la proporzionalità del trattamento e i possibili rischi per i diritti delle persone. La valutazione d’impatto deve contenere anche le mis- ure di sicurezza previste per affrontare i rischi individuati. Per predisporre gli elenchi, le autorità di controllo degli Stati membri sono tenute a cooperare tra loro e con il comitato europeo per la protezione dei dati. Questo garantisce un approccio coerente, in tutta l’UE, alle operazioni che richiedono una valutazi- one d’impatto e i titolari del trattamento saranno soggetti a disposizioni simili indipendentemente dalla loro ubicazione.

Se a seguito di una valutazione d’impatto risulta che il trattamento presenter- ebbe un rischio elevato per i diritti delle persone e in assenza di misure adot- tate per attenuare il rischio, il titolare del trattamento deve consultare l’autorità di controllo competente prima di procedere al trattamento[474].

Il Gruppo di lavoro ar ticolo 29 ha pubblicato linee guida sulle valutazioni d’impatto sulla protezione dei dati e come determinare la possibilità che il trat- tamento possa o meno presentare un rischio elevato[475]. Esso ha elaborato nove criteri per determinare se in un caso specifico sia necessaria una valutazione d’impatto sulla protezione dei dati[476]: 1) valutazione o assegnazione di un pun- teggio; 2) processo decisionale automatizzato che ha

effetto giuridico o incide in modo analogo significativamente; 3) monitoraggio sistematico; 4) dati sensibili;
5) trattamento di dati su larga scala; 6) creazione di corrispondenze o combina- zioni di insiemi di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di soluzioni tecnologiche o organizzative; 9) quando il trattamento in sé «impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto». Il Gruppo di lavoro articolo 29 ha introdotto la regola per cui i trattamenti che soddisfano meno di due criteri presentano un livello di rischio meno elevato e non richiedono una valutazione d'impatto sulla protezione dei dati, mentre i trattamenti che soddisfano due o più criteri richiederanno tale val- utazione. Nei casi in cui non è chiaro se sia richiesta una valutazione di impatto sulla protezione dei dati, il Gruppo di lavoro articolo 29 raccomanda di effettu- arla comunque in quanto detta valutazione è «uno strumento utile che assiste i

titolari del trattamento a rispettare la legge in materia di protezione dei dati»[477]. Qualora entri in uso una nuova tecnologia di trattamento dei dati, è importante che sia effettuata una valutazione di impatto sulla protezione dei dati[478].

4.3.4. Codici di condotta

I codici di condotta sono destinati a essere utilizzati in diversi settori indus- triali, per delineare e precisare l'applicazione del RGPD nei settori specifici. Per i titolari del trattamento e i responsabili del trattamento, la creazione di tali codici può migliorare significativamente il rispetto e l'attuazione delle norme dell'UE in materia di protezione dei dati. Le competenze degli operatori del settore possono favorire l'individuazione di soluzioni pratiche e, pertanto, di probabile applicazione. Riconoscendo l'importanza di tali codici nell'effettiva applicazione della normativa sulla protezione dei dati, il RGPD invita gli Stati membri, le autorità di controllo, la Commissione e il comitato europeo per la protezione dei dati a incoraggiare l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del regolamento in tutta l'UE[479]. I codici potrebbero precisare l'applicazione del regolamento in settori specifici, tra cui la raccolta dei dati personali, le informazioni da fornire agli interessati e al pub- blico e l'esercizio dei diritti degli interessati.

Per garantire che siano conformi alle norme stabilite nel quadro del RGPD, i codici di condotta devono essere sottoposti all'autorità di controllo compe- tente prima di essere adottati. L'autorità di controllo esprime quindi un parere sulla conformità al regolamento del progetto di codice e approva il codice se ritiene che offra garanzie adeguate[480]. Le autorità di controllo devono pub- blicare i codici di condotta approvati, nonché i criteri sui quali si è basata la loro approvazione. Se un progetto di codice di condotta si riferisce alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modi- fica o la proroga, l'autorità di controllo competente lo sottopone al comitato europeo per la protezione dei dati, il quale formula un parere sulla conformità del codice al RGPD. La Commissione può decidere, mediante atti di esecuzione, che il codice di condotta approvato ha validità generale all'interno dell'Unione.

L'adesione a un codice di condotta offre vantaggi significativi sia agli interessati sia ai titolari e ai responsabili del trattamento. Tali codici forniscono orientamenti

dettagliati che adattano i requisiti di legge a settori specifici e promuovono la trasparenza delle attività di trattamento. I titolari del trattamento e i respon- sabili del trattamento possono inoltre utilizzare l'adesione ai codici come prova a dimostrazione della loro conformità con il diritto dell'UE e come mezzo per rafforzare la loro immagine pubblica in quanto organizzazioni che attribuiscono la priorità alla protezione dei dati e si impegnano in tal senso nello svolgimento delle loro attività. Codici di condotta approvati, unitamente a impegni vincolanti ed esecutivi, potrebbero essere utilizzati come garanzie adeguate per il trasferi- mento dei dati verso paesi terzi. Per garantire che le organizzazioni aderenti ai codici di condotta vi si conformino di fatto, può essere designato un organismo speciale (accreditato dall'autorità di controllo competente) incaricato di con- trollarne e garantirne il rispetto. Per assolvere efficacemente i propri compiti, l'organismo deve essere indipendente e competente riguardo alle questioni dis- ciplinate dal codice di condotta e deve disporre di procedure e strutture traspar- enti, che gli consentono di gestire i reclami relativi a violazioni del codice[481].

Nell'ambito del diritto del CdE, la Convenzione n. 108 modernizzata prevede che il livello di protezione dei dati garantito dalla legislazione nazionale possa essere utilmente rafforzato da misure di regolamentazione su base volontaria, quali i codici buone prassi o i codici di condotta professionale.

Tuttavia, si tratta solo di misure volontarie ai sensi della Convenzione n. 108 modernizzata: non si può derivare alcun obbligo giuridico di mettere in atto tali misure, anche se è auspicabile, e tali misure non sono di per sé sufficienti a garantire la piena osservanza della Convenzione[482].

4.3.5. Certificazione

Oltre ai codici di condotta, i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati costituiscono un altro mezzo attraverso il quale i titolari del trattamento e i responsabili del trattamento possono dimostrare la conformità al RGPD. A tal fine, il regolamento prevede un sistema di certificazione volon- taria, in base al quale determinati organismi o autorità di controllo possono rilas- ciare certificazioni. I titolari del trattamento i responsabili del trattamento che scelgono di aderire a un meccanismo di certificazione possono ottenere mag- giore visibilità e credibilità, dal momento che le certificazioni, i sigilli e i marchi consentono agli interessati di valutare rapidamente il livello di protezione dei dati di un'organizzazione ai fini del trattamento dei dati. Di conseguenza, il fatto

che un titolare di trattamento o un responsabile di trattamento sia in possesso di tale certificazione non riduce i suoi compiti e le sue responsabilità ai fini della conformità con tutti gli obblighi previsti dal regolamento.

4.4. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Protezione dei dati fin dalla progettazione

Il diritto dell'UE prescrive che i titolari del trattamento mettano in atto misure per attuare in modo efficace i principi di protezione dei dati e integrare le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati[483]. Tali misure dovrebbero essere attuate sia all'atto del trattamento sia al momento di determinare i mezzi dello stesso. Nell'attuare tali misure il tito- lare del trattamento deve tenere conto dello stato dell'arte, dei costi di attuazi- one, della natura, dell'oggetto e delle finalità del trattamento di dati personali, come anche dei rischi e della gravità per i diritti e le libertà degli interessati[484].

Il diritto del CdE prescrive che i titolari del trattamento e i responsabili del trat- tamento valutino, prima dell'inizio dell'attività di trattamento, il probabile effetto del trattamento dei dati personali sui diritti e sulle libertà degli interessati. Inoltre, i titolari e i responsabili del trattamento sono tenuti a progettare

il trattamento dei dati in modo da minimizzare i rischi di ingerenza in tali diritti e libertà e a implementare misure tecniche e organizzative che tengano conto del diritto alla protezione dei dati personali in tutte le fasi del trattamento[485].

Protezione dei dati per impostazione predefinita

Il diritto dell'UE impone al titolare del trattamento di mettere in atto misure adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari ai fini del trattamento. Tale obbligo vale per la quantità

dei dati personali raccolti, la portata del trattamento, il periodo di conservazi- one e l'accessibilità[486]. Una tale misura deve garantire, ad esempio, che non tutti i dipendenti dei titolari del trattamento abbiano accesso ai dati personali degli interessati. Il GEPD ha elaborato ulteriori orientamenti in un pacchetto di strumenti per la gestione delle esigenze, il *Necessity Toolkit*[487].

Il diritto del CdE prescrive che i titolari e i responsabili del trattamento adot- tino misure tecniche e organizzative tenendo conto delle implicazioni del diritto alla protezione dei dati e a implementare misure tecniche e organizzative che tengano conto del diritto alla protezione dei dati personali in tutte le fasi del trattamento[488].

Nel 2016 l'ENISA ha pubblicato una relazione sugli strumenti e sui servizi in materia di vita privata attualmente disponibili[489]. Tra le altre considerazioni, tale valutazione fornisce un indice di criteri e parametri che sono indicatori di buone o cattive pratiche in materia di riservatezza. Mentre alcuni criteri riguardano direttamente le disposizioni del RGPD, come ad esempio il ricorso alla pseudoni- mizzazione e a meccanismi di certificazione approvati, altri forniscono iniziative innovative per garantire la protezione della vita privata fin dalla progettazione e la protezione per impostazione predefinita. Per esempio, il criterio dell'usabilità, pur non essendo direttamente connesso alla vita

privata, potrebbe migliorare il livello di riservatezza, dal momento che può consentire l'adozione più ampia di uno strumento o di un servizio a tutela della vita privata. In effetti, gli stru- menti a tutela della vita privata di difficile attuazione potrebbero, nella pratica, avere un livello di adozione molto basso presso il pubblico generale, anche se offrono solide garanzie per la vita privata. Inoltre, il criterio della maturità e della stabilità dello strumento a tutela della vita privata, cioè il modo in cui uno strumento evolve nel tempo e risponde alle sfide, nuove o esistenti, legate alla vita privata, è di importanza fondamentale. Altre tecnologie per il raffor- zamento della vita privata ad esempio, nel contesto delle comunicazioni sicure, comprendono la cifratura da punto a punto (comunicazione in cui le uniche persone che possono leggere i messaggi sono le persone che comunicano); la cifratura client-server (cifratura del canale di comunicazione tra client e server); l'autenticazione (verifica dell'identità delle parti che comunicano) e la comuni- cazione anonima (nessun terzo può identificare le parti che comunicano).

- Il controllo indipendente è un elemento essenziale del diritto europeo in materia di protezione dei dati ed è sancito dall'articolo 8, paragrafo 3, della Carta.

- Per garantire un'effettiva protezione dei dati devono essere create autorità di controllo indipendenti ai sensi della normativa nazionale.

- Le autorità di controllo devono agire in assoluta indipendenza, garantita dalla legge che le istituisce e ripresa nella specifica struttura organizzativa dell'autorità di controllo.

- Le autorità di controllo hanno competenze e funzioni specifiche, fra cui:

- controllare e promuovere la protezione dei dati a livello nazionale;

- fornire pareri agli interessati e ai titolari del trattamento nonché al governo e al pubblico in senso lato;

- ricevere i reclami e assistere gli interessati in caso di presunte violazioni dei diritti in materia di protezione dei dati;

- vigilare sui titolari e sui responsabili del trattamento.

- Le autorità di controllo hanno altresì il potere di intervenire, se necessario:

- avvertendo, ammonendo o persino sanzionando titolari e responsabili del trattamento,

- ordinando la rettifica, il blocco del trattamento o la cancellazione dei dati;

- imponendo un divieto sul trattamento o una sanzione amministrativa;

- deferendo questioni all'autorità giudiziaria.

- Poiché il trattamento dei dati personali spesso coinvolge titolari del trattamento, responsabili del trattamento e interessati, situati in Stati diversi, le autorità di controllo sono tenute a cooperare tra loro sulle questioni transfrontaliere, per garantire un'efficace protezione delle persone in Europa.

- Nell'ambito dell'UE, il regolamento generale sulla protezione dei dati istituisce un meccanismo di sportello unico per i casi riguardanti il trattamento transfrontaliero. Alcune aziende svolgono attività di trattamento transfrontaliero in ragione del trat- tamento di dati personali che ha

luogo nell’ambito delle attività di stabilimenti in più di uno Stato membro o nell’ambito di un unico stabilimento nell’Unione ma che incide in modo sostanziale su interessati di più di uno Stato membro. Nell’ambito del meccanismo, tali aziende dovranno trattare con un’unica autorità nazionale di controllo per la protezione dei dati.

• Un meccanismo di cooperazione e coerenza permetterà un approccio coordinato tra tutte le autorità di controllo coinvolte nel caso. L’autorità di controllo capofila,

dello stabilimento principale o dello stabilimento unico, consulterà le altre autorità di controllo interessate e trasmetterà loro il suo progetto di decisione.

•	Analogamente all'attuale Gruppo di lavoro articolo 29, l'autorità di controllo di ciascuno Stato membro e il Garante europeo della protezione dei dati (GEPD) far- anno parte del comitato europeo per la protezione dei dati.

•	I compiti del comitato europeo per la protezione dei dati comprendono, ad esem- pio, la sorveglianza della corretta applicazione del regolamento, fornire consu- lenza alla Commissione in merito a questioni pertinenti e formulare pareri, linee guida o migliori prassi su una varietà di argomenti.

•	La principale differenza consiste nel fatto che il comitato europeo per la pro- tezione dei dati non si limiterà a emettere pareri, come previsto dalla direttiva
95/46/CE. Esso emetterà anche decisioni vincolanti nei casi in cui un'autorità di controllo abbia sollevato un'obiezione pertinente e motivata riguardante casi di sportello unico; qualora esistano pareri divergenti riguardo a quale autorità di controllo sia capofila e, infine, quando l'autorità di controllo non richiede o non si conforma al parere del comitato europeo per la

protezione. L'obiettivo è garantire un'applicazione coerente del regolamento in tutti gli Stati membri.

Il controllo indipendente è un elemento essenziale del diritto europeo in materia di protezione dei dati. Il diritto dell'UE e il diritto del CdE considerano l'esistenza di autorità di controllo indipendenti indispensabile per la tutela effettiva dei diritti e delle libertà delle persone, per quanto riguarda il trattamento dei loro dati personali. Poiché oggi il trattamento dei dati è più che mai presente e sempre più complesso da comprendere per le persone, tali autorità sono i custodi dell'era digitale. Nell'UE l'esistenza di autorità di controllo indipendenti è con- siderata uno degli elementi fondamentali del diritto alla protezione dei dati per- sonali, sancito dal diritto primario dell'UE. L'articolo 8, paragrafo 3, della Carta dei diritti fondamentali dell'UE e l'articolo 16, paragrafo 2, del TFUE riconoscono la protezione dei dati personali come diritto fondamentale e stabiliscono che il rispetto delle norme in materia di protezione dei dati deve essere assoggettato al controllo di un'autorità indipendente.

L'importanza di un controllo indipendente per la normativa in materia di pro- tezione dei dati è stata riconosciuta anche nella giurisprudenza.

Esempio: nella causa *Schrems*[490], la CGUE è stata chiamata a decidere se il trasferimento di dati

personali verso gli Stati Uniti (USA), nell’ambito del primo

accordo UE-USA basato sui principi di approdo sicuro, fosse o meno conforme al diritto europeo in materia di protezione dei dati, alla luce delle rivelazioni di Edward Snowden sulla condotta dell’agenzia National Security Agency degli Stati Uniti, con riferimento alla sorveglianza di massa. Il trasferimento dei dati personali verso gli Stati Uniti era basato su una decisione della Commissione europea, adottata nel 2000, che permetteva di trasferire dati personali dall’UE verso organizzazioni statunitensi che autocertificano la loro adesione al regime dell’approdo sicuro, sulla base del fatto che tale regime garantisce un livello adeguato di protezione dei dati personali. Alla richiesta di esaminare la denuncia del ricorrente sulla legittimità dei trasferimenti dei dati dopo le rivelazioni di Snowden, l’autorità di controllo irlandese aveva respinto la denuncia con la motivazione che l’esistenza della decisione della Commissione sull’adeguatezza del regime statunitense di protezione dei dati, ispirata ai principi di approdo sicuro (decisione «approdo sicuro») ostava a che la stessa istruisse ulteriormente la denuncia.

La CGUE ha tuttavia stabilito che l’esistenza di una decisione della Commissione, che consente i trasferimenti di dati verso paesi terzi che garantiscono livelli adeguati di protezione, non elide né riduce i poteri delle autorità nazionali di controllo. La CGUE ha osservato che i poteri di tali

autorità di controllare e assicurare il rispetto della normativa dell'UE in materia di protezione dei dati risultano dal diritto primario dell'UE, segnatamente l'articolo 8, paragrafo 3, della Carta e l'articolo 16, paragrafo 2, del TFUE. «L'istituzione [...] di autorità di controllo indipendenti costituisce quindi [...] un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali»[491].

La CGUE ha pertanto deciso che, anche qualora il trasferimento dei dati personali sia stato oggetto di una decisione della Commissione sull'adeguatezza, se un'autorità nazionale di controllo è investita di una denuncia, incombe a detta autorità esaminare la denuncia con diligenza. L'autorità di controllo può respingere la denuncia se la ritiene priva di fondamento. Nella fattispecie, la CGUE ha sottolineato che il diritto a una tutela giurisdizionale effettiva esige che tali persone siano in grado di contestare siffatta decisione dinanzi ai tribunali nazionali, i quali possono investire la CGUE di un procedimento pregiudiziale per un accertamento di validità della decisione della Commissione. Se ritiene fondata la domanda,

l'autorità di controllo deve poter promuovere azioni giudiziarie e far valere la questione dinanzi ai giudici nazionali. Questi ultimi possono deferire la causa alla CGUE, che è l'unico organo competente a decidere in merito alla validità di una decisione della Commissione sull'adeguatezza[492].

La CGUE ha quindi esaminato la validità della decisione «approdo sicuro», onde determinare se il sistema dei trasferimenti fosse o meno conforme alle norme dell'UE in materia di protezione dei dati. Essa ha constatato che l'articolo 3 della decisione «approdo sicuro» limitava i poteri delle autorità nazionali di controllo (conferiti dalla direttiva sulla tutela dei dati) di adottare misure per impedire i trasferimenti di dati in caso di livello di protezione inadeguato dei dati personali negli Stati Uniti. In considerazione dell'importanza delle autorità di controllo indipendenti nel garantire il rispetto del diritto in materia di protezione dei dati, la CGUE ha stabilito che, in virtù della direttiva sulla tutela dei dati alla luce della Carta, la Commissione non aveva la competenza per limitare in tal modo i poteri delle autorità di controllo indipendenti. La limitazione dei poteri delle autorità di controllo era una delle ragioni per cui la CGUE ha dichiarato l'invalidità della decisione «approdo sicuro».

Il diritto europeo impone, pertanto, un controllo indipendente quale impor- tante meccanismo per

garantire un’effettiva protezione dei dati. Le autorità di controllo indipendenti sono il primo punto di contatto per gli interessati in caso di violazioni della vita privata[493]. Nell’ambito del diritto dell’UE e del CdE, l’istituzione di autorità di controllo è obbligatoria. Entrambi i quadri giuridici descrivono i compiti e i poteri di tali autorità in modo simile al RGPD. In linea di principio, le autorità di controllo dovrebbero, pertanto, funzionare allo stesso modo nell’ambito del diritto dell’UE e del CdE[494].

5.1. Indipendenza

Il diritto dell’UE e il diritto del CdE impongono a ogni autorità di con- trollo di agire in piena indipendenza nell’adempimento dei propri compiti e nell’esercizio dei propri poteri[495]. L’indipendenza dell’autorità di controllo, dei

suoi membri e del suo personale, da pressioni esterne dirette o indirette, è fondamentale per garantire la massima obiettività al momento di decidere su questioni concernenti la protezione dei dati. Non è solo la legislazione in base alla quale è istituita l'autorità di controllo a dover contenere disposizioni atte a garantirne l'indipendenza, ma è anche la particolare struttura organiz- zativa dell'autorità stessa a dover dare prova di tale indipendenza. Nel 2010, la CGUE ha esaminato per la prima volta il grado di indipendenza necessaria alle autorità di controllo per la protezione dei dati[496]. Gli esempi evidenziati illus- trano la definizione attribuita dalla CGUE ai termini «piena indipendenza».

Esempio: nella causa *Commissione europea c. Repubblica federale di Germania*[497], la Commissione europea aveva chiesto alla CGUE di dichiarare che la Germania aveva trasposto erroneamente il requisito secondo cui le autorità di controllo della protezione dei dati devono essere «pienamente indipendenti», venendo meno così agli obblighi a essa incombenti in virtù dell'articolo 28, paragrafo 1, della direttiva sulla tutela dei dati. Secondo la Commissione, il fatto che la Germania, per garantire la conformità con il diritto in materia di protezione dei dati, avesse sottoposto alla vigilanza dello Stato le autorità preposte ai controlli sul trattamento dei dati nei vari Stati federali (*Länder*),

costituiva una violazione del requisito dell'indipendenza.

La CGUE ha sottolineato che i termini «pienamente indipendenti» devono essere interpretati in base al tenore letterale effettivo di tale disposizione nonché alle finalità e all'economia della direttiva europea sulla protezione dei dati[498]. La CGUE ha evidenziato che le autorità di controllo sono «custodi» dei diritti correlati al trattamento dei dati personali. Pertanto, la loro designazione negli Stati membri è considerata «un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali»[499]. La CGUE ha concluso che «nello svolgimento delle loro funzioni, le autorità di controllo devono agire in modo obiettivo ed imparziale. A tale fine esse devono essere

sottratte a qualsiasi influenza esterna, compresa quella, diretta o indiretta, delle autorità pubbliche»[500].

La CGUE ha altresì ritenuto che il significato dei termini «pienamente indipendenti» debba essere interpretato alla luce dell'indipendenza del GEPD, definita nel regolamento sulla protezione dei dati delle istituzioni dell'UE. In tale regolamento, la nozione di indipendenza stabilisce che il GEPD non può sollecitare né accettare istruzioni da alcuno.

Di conseguenza, la CGUE ha statuito che le autorità di controllo in Germania, non erano totalmente indipendenti ai sensi del diritto europeo in materia di protezione dei dati, perché sottoposte alla vigilanza di autorità pubbliche.

Esempio: nella causa *Commissione europea c. Repubblica austriaca*[501], la CGUE ha evidenziato problemi simili per quanto riguarda l'indipendenza di taluni membri e del personale dell'autorità di controllo austriaca (commissione per la protezione dei dati, DSK). La CGUE ha concluso che il fatto che la cancelleria federale fornisse il personale all'autorità di controllo, comprometteva il requisito di indipendenza previsto dal diritto dell'UE in materia di protezione dei dati. La CGUE ha stabilito inoltre che l'obbligo di informare la cancelleria in qualsiasi momento sulla propria

attività comprometteva la totale indipendenza dell'autorità di controllo.

Esempio: nella causa *Commissione europea c. Ungheria*[502], pratiche nazionali simili con ripercussioni sulla forza lavoro sono state vietate. La CGUE ha sottolineato che «il requisito [...] secondo il quale deve essere garantito che ogni autorità di controllo sia pienamente indipendente nell'esercizio delle funzioni che le sono attribuite, implichi l'obbligo, per lo Stato membro interessato, di rispettare la durata del mandato di tale autorità fino al termine inizialmente previsto». La CGUE ha inoltre constatato che «ponendo anticipatamente fine al mandato dell'autorità di controllo per la protezione dei dati personali, l'Ungheria è venuta meno agli obblighi ad essa incombenti in forza della direttiva 95/46 [...]».

La nozione e i criteri di «piena indipendenza» sono ora esplicitamente previsti nel RGPD, che incorpora i principi stabiliti nelle citate sentenze della CGUE. Ai sensi del regolamento, la piena indipendenza nell'esecuzione dei loro compiti e nell'esercizio dei loro poteri comporta quanto segue[503]:

- i membri di ogni autorità di controllo non devono subire pressioni esterne, né dirette né indirette, e non devono accettare istruzioni da alcuno;

- i membri di ogni autorità di controllo devono astenersi da qualunque azione incompatibile con le loro funzioni, per evitare conflitti di interesse;

- gli Stati membri devono dotare ogni autorità di controllo delle risorse umane, tecniche e finanziarie e delle infrastrutture necessarie per l'effettivo adempimento dei loro compiti;

- gli Stati membri devono provvedere affinché ogni autorità di controllo selezioni il proprio personale;

- il controllo finanziario al quale ogni autorità di controllo è soggetta ai sensi del diritto nazionale, non deve pregiudicarne l'indipendenza. Le autorità di controllo devono disporre di bilanci annuali separati e pubblici, che consen- tano loro di operare correttamente.

L’indipendenza delle autorità di controllo è considerata un requisito fondamen- tale anche ai sensi del diritto del CdE. La Convenzione n. 108 modernizzata pre- scrive alle autorità di controllo di «agire con indipendenza e imparzialità nello svolgimento delle loro funzioni e nell’esercizio dei loro poteri», senza solleci- tare né accettare istruzioni[504]. In tal modo, la Convenzione riconosce che dette autorità non possono efficacemente salvaguardare i diritti e le libertà delle persone con riguardo al trattamento dei dati, se non esercitano le loro funzioni in completa indipendenza. La relazione esplicativa della Convenzione n. 108 modernizzata definisce una serie di elementi che contribuiscono a salvaguard- are tale indipendenza. Tali elementi includono la possibilità per le autorità di controllo di assumere il proprio personale e di adottare decisioni senza essere soggette a ingerenze esterne nonché fattori relativi alla durata dell’esercizio

delle loro funzioni e le condizioni in presenza delle quali tali funzioni potreb- bero cessare[505].

5.2. Competenze e poteri

Nell'ambito del diritto dell'UE, il RGPD delinea le competenze e la struttura organiz zativa delle autorità di controllo e dispone che siano competenti a eseguire i compiti assegnati e a esercitare i poteri a esse conferiti dal regolamento.

L'autorità di controllo è l'organo principale, nel diritto nazionale, che assi- cura il rispetto del diritto dell'UE in materia di protezione dei dati. Le autorità di controllo hanno una serie completa di compiti e poteri, che vanno oltre il controllo e che comprendono attività di monitoraggio proattive e preventive. Per svolgere tali compiti, le autorità di controllo devono disporre di adeguati poteri di indagine, correttivi e consultivi, elencati all'articolo 58 del RGPD[506], ad esempio:

- fornire consulenza ai titolari del trattamento e agli interessati su tutte le questioni inerenti alla tutela dei dati;

- autorizzare clausole contrattuali tipo, norme vincolanti d'impresa o accordi amministrativi;

- svolgere attività ispettive sulle operazioni di trattamento e intervenire di conseguenza;

- richiedere la comunicazione di tutte le informazioni rilevanti per la sorvegli- anza delle attività di controllo;

- rivolgere avvertimenti o ammonimenti ai titolari del trattamento e ordinare la notificazione di violazioni dei dati personali agli interessati;

- ordinare la rettifica, il blocco del trattamento, la cancellazione o la distruzi- one dei dati;

- imporre un divieto provvisorio o definitivo al trattamento o infliggere san- zioni amministrative;

- deferire una questione all'autorità giudiziaria.

Per poter esercitare le proprie funzioni, un'autorità di controllo deve avere accesso a tutti i dati personali e a tutte le informazioni necessarie a fini d'indagine nonché a tutti i locali in cui un titolare del trattamento conservi informazioni rile- vanti. Secondo la CGUE, i poteri dell'autorità di controllo devono essere interpre- tati estensivamente, per garantire la piena efficacia della protezione dei dati per gli interessati nell'UE.

Esempio: nella causa *Schrems*, la CGUE è stata chiamata a decidere se il trasferimento di dati personali verso gli Stati Uniti nell'ambito del primo accordo UE-USA basato sui principi di «approdo sicuro», fosse conforme al diritto dell'UE in materia di protezione dei dati, alla luce delle rivelazioni di Edward Snowden. Nel suo ragionamento, la CGUE ha affermato che le autorità nazionali di controllo che agiscono in veste di controllori indipendenti del trattamento dei dati effettuato da titolari del trattamento, possono impedire il trasferimento dei dati personali verso un paese terzo, malgrado l'esistenza di una decisione di adeguatezza, qualora sia ragionevolmente provato che la protezione adeguata non è più garantita nel paese terzo[507].

Ogni autorità di controllo è competente a esercitare poteri di inter vento e poteri di indagine all'interno del proprio territorio. Tuttavia, dal momento che le attività dei titolari del trattamento e dei responsabili del trattamento hanno spesso carattere transfrontaliero e che il trattamento dei dati influisce su inter- essati ubicati in diversi Stati membri, sorge la questione della divisione delle competenze tra le diverse autorità di controllo. La CGUE ha avuto l'opportunità di esaminare tale questione nella causa *Weltimmo*.

Esempio: nella causa *Weltimmo*[508], la CGUE è stata chiamata a decidere sulla competenza delle autorità nazionali di controllo nel trattare questioni

concernenti organizzazioni non stabilite nell’ambito della loro giurisdizione. Weltimmo era una società con sede in Slovacchia, che gestiva un sito Internet di annunci immobiliari riguardanti beni situati in Ungheria. Gli inserzionisti avevano presentato reclamo presso l’autorità ungherese di controllo dei dati per violazione della legge ungherese sulla protezione dei dati e l’autorità aveva imposto un’ammenda alla società Weltimmo. La società aveva contestato l’ammenda dinanzi ai giudici nazionali e la causa era stata rinviata alla CGUE affinché stabilisse se la direttiva dell’UE sulla tutela dei dati consentisse alle autorità di controllo di uno Stato membro di applicare la legislazione nazionale in materia di protezione dei dati a una società avente sede in un altro Stato membro.

La CGUE ha interpretato l’articolo 4, paragrafo 1, lettera a), della direttiva sulla tutela dei dati nel senso che consentiva l’applicazione della legge in materia di protezione dei dati in uno Stato membro diverso da quello nel quale il titolare del trattamento è registrato, «purché il medesimo svolga, tramite un’organizzazione stabile nel territorio di tale Stato membro, un’attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento». La CGUE ha osservato, sulla base delle informazioni fornitele, che la Weltimmo svolgeva un’attività concreta ed effettiva in Ungheria, dal momento

che aveva un rappresentante in Ungheria, il quale figurava nel registro slovacco delle società a un indirizzo situato in Ungheria, disponeva di un conto bancario e di una casella postale ungheresi, e svolgeva inoltre attività in Ungheria in lingua ungherese. Tali informazioni erano indicative dell'esistenza di uno stabilimento e rendevano l'attività della Weltimmo soggetta alla legislazione ungherese sulla protezione dei dati e alla giurisdizione dell'autorità di controllo ungherese. Tuttavia, la CGUE ha lasciato al giudice nazionale il compito di verificare le informazioni e determinare se Weltimmo disponesse di fatto di uno stabilimento in Ungheria.

Se il giudice del rinvio avesse ritenuto che Weltimmo disponeva di uno stabilimento in Ungheria, l'autorità di controllo ungherese avrebbe avuto potere sanzionatorio. Tuttavia, qualora il giudice nazionale avesse deciso il contrario, vale a dire che Weltimmo non disponeva di uno stabilimento in Ungheria, il diritto applicabile sarebbe stato, di conseguenza, quello dello Stato membro o degli Stati membri nei quali la società era registrata. Nella fattispecie, dal momento che i poteri delle autorità di controllo devono essere esercitati nel rispetto della sovranità territoriale degli altri Stati membri, l'autorità ungherese non avrebbe potuto imporre sanzioni. Poiché la direttiva

sulla tutela dei dati prevedeva un obbligo di cooperazione per le autorità di controllo, l'autorità di controllo ungherese poteva, tuttavia, richiedere alla sua omologa slovacca di esaminare la questione, accertare un'eventuale violazione della legislazione slovacca e imporre le sanzioni previste da tale legislazione.

A seguito dell'adozione del RGPD sono attualmente in vigore norme dettagliate sulla competenza delle autorità di controllo nelle controversie transfrontaliere. Il regolamento prevede un «meccanismo dello sportello unico» e contiene dispo- sizioni che impongono la cooperazione tra diverse autorità di controllo. Ai fini di una cooperazione efficace nei casi transfrontalieri, il RGPD prevede l'istituzione di un'autorità di controllo capofila competente ad agire in qualità di autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare o del responsabile del trattamento[509]. L'autorità di controllo capofila è competente per la gestione delle cause transfrontaliere, è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento e coordina la cooperazione con altre autorità di controllo al fine di raggiungere un consenso. La cooperazi- one comprende lo scambio di informazioni, l'assistenza reciproca nel controllo e nello svolgimento di indagini e l'adozione di decisioni vincolanti[510].

Nell’ambito del diritto del CdE, le competenze e i poteri delle autorità di con- trollo sono previste dall’articolo 15 della Convenzione n. 108 modernizzata. Tali poteri corrispondono a quelli conferiti alle autorità di controllo in virtù del diritto dell’UE, compresi poteri di indagine e di intervento, poteri di adottare decisioni e imporre sanzioni amministrative concernenti violazioni delle dispo- sizioni della Convenzione e poteri di intentare azioni. Le autorità di controllo indipendenti dispongono altresì della competenza di trattare richieste e rec- lami proposti dagli interessati, per sensibilizzare il pubblico sulla legislazione in materia di protezione dei dati e fornire consulenza agli organi decisionali nazi- onali con riferimento a misure legislative o amministrative che prevedono il trattamento dei dati personali.

5.3. Cooperazione

Il RGPD stabilisce un quadro generale per la cooperazione tra le autorità di controllo e prevede norme più specifiche sulla cooperazione tra le stesse nelle attività transfrontaliere e di trattamento dei dati.

Ai sensi del RGPD, le autorità di controllo si prestano assistenza reciproca e si scambiano informazioni utili al fine di attuare e applicare il regolamento in maniera coerente[511]. Questo comprende l'effettuazione di consultazioni, ispezioni e indagini da parte dell'autorità di controllo interpellata. Le autorità di controllo possono condurre operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipa il personale di tutte le autorità di controllo coinvolte.[512]

Nell'UE, i titolari del trattamento e i responsabili del trattamento operano sem- pre più a livello transnazionale. Ciò presuppone una stretta cooperazione tra le autorità di controllo competenti negli Stati membri, al fine di assicurare che il trattamento dei dati personali sia conforme alle prescrizioni del RGPD. In base al meccanismo dello «sportello unico», qualora un titolare del trattamento o responsabile del trattamento sia stabilito in diversi Stati membri o qualora abbia uno stabilimento unico ma le operazioni di trattamento

incidono in modo sostanziale su interessati di più di uno Stato membro, l’autorità di controllo dello stabilimento principale (o unico) funge da autorità capofila per le attività transfrontaliere del titolare del trattamento o del responsabile del trattamento. Le autorità capofila possono adottare misure di contrasto nei confronti del titolare del trattamento o responsabile del trattamento. Il meccanismo dello sportello unico è volto a migliorare l’armonizzazione e l’applicazione uniforme della legislazione dell’UE in materia di protezione dei dati in diversi Stati mem- bri. Esso è vantaggioso anche per le aziende, in quanto devono trattare solo con l’autorità capofila, anziché con diverse autorità di controllo. Ciò migliora la certezza del diritto per le aziende e, nella pratica, dovrebbe anche signifi- care che le decisioni sono adottate con maggiore rapidità e che le aziende non devono interloquire con autorità di controllo diverse, che impongono loro pre- scrizioni contrastanti.

L’individuazione dell’autorità capofila implica la determinazione dell’ubicazione dello stabilimento principale di un’azienda nell’UE. Il termine «stabilimento

principale» è definito nel RGPD. Inoltre, il Gruppo di lavoro articolo 29 ha pub- blicato linee guida per l'identificazione dell'autorità di controllo capofila in relazione a un titolare del trattamento o responsabile del trattamento, che comprendono i criteri per l'individuazione dello stabilimento principale[513].

Per garantire un livello di protezione dei dati elevato in tutta l'UE, l'autorità di controllo capofila non agisce da sola. Deve cooperare con le altre autorità di controllo interessate per adottare decisioni sul trattamento dei dati personali da parte di titolari responsabili del trattamento, al fine di raggiungere un con- senso e garantire la coerenza. La cooperazione tra le autorità di controllo inter- essate comprende lo scambio di informazioni, l'assistenza reciproca, lo svolgi- mento di indagini congiunte e il controllo di attività[514]. Nel prestarsi assistenza reciproca, le autorità di controllo devono gestire con precisione le richieste di informazioni provenienti da altre autorità di controllo, nonché attuare misure di controllo come, ad esempio, autorizzazioni preventive e consultazioni con il titolare del trattamento in merito alle sue attività di trattamento, ispezioni o indagini. L'assistenza reciproca alle autorità di controllo in altri Stati membri deve essere prestata su richiesta, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa[515].

Qualora il titolare del trattamento abbia stabilimenti in vari Stati membri, le autorità di controllo possono condurre operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipano membri o personale di autorità di controllo di altri Stati membri[516].

La cooperazione tra le diverse autorità di controllo è un requisito importante anche ai sensi del diritto del CdE. La Convenzione n. 108 modernizzata prevede che le autorità di controllo cooperino tra loro nella misura necessaria per l'adempimento delle loro funzioni[517]. A tal fine esse dovrebbero, ad esempio, scambiarsi informazioni pertinenti e utili, coordinare le indagini ed effettuare azioni comuni[518].

5.4. Il comitato europeo per la protezione dei dati

L'importanza delle autorità di controllo indipendenti e le principali competenze di cui esse dispongono ai sensi del diritto europeo in materia di protezione dei dati, sono state descritte in precedenza in questo capitolo. Il comitato europeo per la protezione dei dati (CEPD) è un altro attore importante che assicura che le norme sulla protezione dei dati siano applicate in modo efficace e coerente in tutta l'UE.

Il RGPD ha istituito il CEPD quale organismo dotato di personalità giuridica[519]. È il successore del Gruppo di lavoro articolo 29[520], istituito dalla direttiva sulla tutela dei dati per consigliare la Commissione su qualsiasi misura UE che incida sui diritti delle persone fisiche in relazione al trattamento dei dati personali e alla vita privata, per promuovere l'applicazione uniforme della direttiva e per fornire alla Commissione pareri di esperti in materia di protezione dei dati. Il Gruppo di lavoro articolo 29 era composto da rappresentanti delle autorità di controllo degli Stati membri dell'UE e da rappresentanti della Commissione e del GEPD.

Analogamente al Gruppo di lavoro, il CEPD è composto dai vertici delle autorità di controllo per ciascuno Stato membro e dal GEPD, o dai loro rappresentanti[521]. Il GEPD gode di pari diritti di voto, ad eccezione dei casi relativi alla risoluzione delle controversie, in cui può votare solo per decisioni che

riguardano principi e norme applicabili alle istituzioni dell'UE, corrispondenti nella sostanza a quelli del RGPD. La Commissione ha il diritto di partecipare alle attività e alle riunioni del CEPD ma senza diritto di voto[522]. Il comitato elegge un presidente (al quale è affidata la rappresentanza) e due vicepresidenti tra i suoi membri a mag- gioranza semplice, con mandato di cinque anni. Il CEPD dispone, inoltre, di una segreteria messa a disposizione dal GEPD, per fornire al comitato assistenza in materia di analisi, amministrativa e logistica[523].

I compiti del CEPD sono descritti dettagliatamente negli articoli 64, 65 e 70 del RGPD e comprendono compiti generali, che possono essere suddivisi nelle tre attività principali riportate di seguito.

• Coerenza: il CEPD può emettere decisioni giuridicamente vincolanti in tre casi: quando un'autorità di controllo abbia sollevato un'obiezione pertinente e motivata riguardante casi di sportello unico; qualora esistano pareri diver- genti riguardo a quale autorità di controllo sia «capofila» e, infine, quando l'autorità di controllo competente non richiede o non si conforma al parere del CEPD.[524]
La principale responsabilità del CEPD è garantire l'applicazione coerente del RGPD in tutta l'UE ed esso svolge un ruolo fondamentale nel meccanismo di coerenza, come descritto nella sezione 5.5.

• Consultazione: i compiti del CEPD comprendono la consulenza alla Com- missione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, come le modifiche al RGPD, le revisioni della nor- mativa dell'UE che implicano un trattamento dei dati e potrebbero essere in conflitto con le norme dell'UE sulla protezione dei dati o l'adozione da parte della Commissione di decisioni di adeguatezza, che consentano il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale.

- Orientamenti: il comitato pubblica inoltre linee guida, raccomandazioni e migliori prassi per incoraggiare l'applicazione coerente del regolamento e promuove la cooperazione e lo scambio di conoscenze tra le autorità di con- trollo. Inoltre, deve incoraggiare le associazioni di titolari del trattamento o di responsabili del trattamento a elaborare codici di condotta e istituire meccanismi di certificazione della protezione dei dati e sigilli.

Le decisioni del CEPD possono essere impugnate dinanzi alla CGUE.

5.5. Il meccanismo di coerenza del RGPD

Il RGPD istituisce un meccanismo di coerenza onde assicurare che il regola- mento sia applicato in modo coerente in tutti gli Stati membri, mediante il quale le autorità di controllo cooperano tra loro e, eventualmente, con la

Commissione. Il meccanismo di coerenza è utilizzato in due situazioni. La prima riguarda i pareri del CEPD in casi in cui un'autorità di controllo competente intende adottare misure, come un elenco di operazioni di trattamento che rich- iedono una valutazione d'impatto sulla protezione dei dati, o per adottare clau- sole contrattuali tipo. La seconda riguarda le decisioni vincolanti del CEPD per le autorità di controllo nei casi di sportello unico e quando un'autorità di controllo non si conforma a un parere del CEDP o non lo richiede.

L'efficacia delle norme giuridiche in generale e dei diritti degli interessati in particolare dipende, in larga misura, dall'esistenza di meccanismi adeguati per la loro attuazione. Nell'era digitale, il trattamento dei dati si è diffuso capillar- mente e diventa sempre più difficile da comprendere per gli individui. Al fine di ridurre gli squilibri di potere tra gli interessati e i titolari del trattamento, ai singoli sono stati attribuiti determinati diritti affinché possano esercitare un maggiore controllo sul trattamento delle loro informazioni personali. Il diritto di accesso ai propri dati e il diritto di ottenerne la rettifica sono sanciti

dall'articolo 9, paragrafo 2, della Carta dei diritti fondamentali dell'UE, un doc- umento che costituisce il diritto primario dell'UE e assume un valore fonda- mentale nell'ordinamento giuridico dell'Unione. Il diritto derivato dell'UE, in particolare il regolamento generale sulla protezione dei dati, ha istituito un quadro giuridico coerente, che conferisce agli interessati diritti nei confronti dei titolari del trattamento dei dati. Oltre ai diritti di accesso e di rettifica, il RGPD riconosce una serie di altri diritti, come il diritto alla cancellazione («diritto all'oblio»), il diritto di opporsi o di limitare il trattamento dei dati e i diritti rela- tivi ai processi decisionali automatizzati e alla profilazione. Garanzie analoghe, per consentire agli interessati di esercitare un controllo efficace sui propri dati, sono previste anche dalla Convenzione n. 108 modernizzata. L'articolo 8 elenca i diritti che le persone dovrebbero essere in grado di esercitare in relazione al trattamento dei propri dati personali. Le parti contraenti devono garantire che tali diritti siano accessibili a tutti gli interessati nell'ambito della loro giuris- dizione e che siano accompagnati da strumenti giuridici pratici ed efficaci per consentire loro di esercitarli.

Oltre a garantire i diritti delle persone fisiche, è altrettanto importante istituire meccanismi che consentano agli interessati di contestare le violazioni dei loro diritti, ritenere responsabili i titolari del trattamento e chiedere un risarcimento. Il diritto a un

ricorso effettivo, sancito dalla CEDU e dalla Carta, esige che siano messi a disposizione di ognuno mezzi di ricorso giurisdizionali.

6.1. I diritti degli interessati

- Ogni interessato ha il diritto di essere informato sul trattamento dei propri dati personali da parte di qualsiasi titolare del trattamento, fatte salve alcune limitate eccezioni.

- Gli interessati hanno il diritto di:

- accedere ai propri dati e ottenere determinate informazioni circa il trattamento;

- ottenere eventualmente dal titolare del trattamento la rettifica dei propri dati, se i dati sono inesatti;

- ottenere eventualmente dal titolare del trattamento la cancellazione dei pro- pri dati, se il trattamento è illegale;

- limitare temporaneamente il trattamento;

- ottenere il trasferimento dei propri dati a un altro titolare del trattamento, in determinate condizioni.

- Inoltre, gli interessati hanno il diritto di opporsi al trattamento nei seguenti casi:

- motivi che riguardano la loro situazione particolare;

- uso dei loro dati a fini di marketing diretto.

- Gli interessati hanno il diritto di non essere sottoposti a decisioni basate unica- mente sul trattamento automatizzato, compresa la profilazione, che producano effetti giuridici che li riguardano o incidano significativamente sulla loro persona. Gli interessati hanno inoltre il diritto di:

- ottenere l'intervento umano da parte del titolare del trattamento;

• esprimere la propria opinione e contestare una decisione fondata su un trat- tamento automatizzato.

6.1.1. Diritto di essere informati

Ai sensi del diritto del CdE nonché del diritto dell'UE, i titolari delle operazioni di trattamento sono obbligati a informare l'interessato, al momento della raccolta dei dati personali, circa la finalità del trattamento. Quest'obbligo non dipende da una richiesta dell'interessato, ma deve essere rispettato in modo proattivo dal titolare del trattamento, a prescindere dal fatto che l'interessato mostri o meno interesse per le informazioni.

Nell'ambito del diritto del CdE, ai sensi dell'articolo 8 della Convenzione n. 108 modernizzata, le parti contraenti devono prevedere che i titolari del tratta- mento informino gli interessati circa la loro identità e domicilio abituale, la base giuridica e la finalità del trattamento, le categorie di dati personali trattati, i destinatari dei loro dati personali (eventualmente) e i mezzi con cui possono esercitare i diritti di cui all'articolo 9, che comprende i diritti di accesso, ret- tifica e ricorso. Agli interessati deve essere comunicata anche qualsiasi altra informazione supplementare considerata necessaria per assicurare un tratta-

mento corretto e trasparente dei dati personali. La relazione esplicativa della

Convenzione n. 108 modernizzata precisa che le informazioni presentate agli interessati «devono essere facilmente accessibili, leggibili, comprensibili e adattate agli interessati»[525].

Nell'ambito del diritto dell'UE, il principio di trasparenza richiede che qualsiasi trat- tamento di dati personali sia generalmente trasparente per le persone fisiche. Le persone hanno il diritto di conoscere le modalità con cui dati personali sono raccolti, utilizzati o altrimenti trattati, e il loro contenuto, nonché di essere sen- sibilizzate ai rischi, alle garanzie e ai loro diritti relativi al trattamento dei dati[526]. L'articolo 12 del RGPD prevede, pertanto, un ampio obbligo generale, per i titolari del trattamento, di fornire informazioni trasparenti e o comunicare le modalità con cui gli interessati possono esercitare i loro diritti[527]. Le informazioni devono essere concise, trasparenti, comprensibili e facilmente accessibili, e deve essere utilizzato un linguaggio semplice e chiaro. Esse devono essere fornite per iscritto, anche con mezzi elettronici, se appropriato, e possono anche essere fornite oralmente su richiesta dell'interessato, purché la sua identità sia provata al di là di ogni dubbio. Le informazioni devono essere fornite senza ritardi o costi eccessivi[528].

L'articolo 13 e l'articolo 14 del RGPD riguardano, rispettivamente, il diritto degli interessati di essere informati in situazioni in cui i dati personali sono stati

rac- colti direttamente presso gli stessi o in situazioni in cui i dati non sono stati otte- nuti dagli interessati.

La portata del diritto all'informazione e i suoi limiti ai sensi del diritto dell'UE
sono stati precisati nella giurisprudenza della CGUE.

Esempio: nella causa *Institut. Professionnel des agents Immobiliers (IPI) c. Englebert*[529], alla CGUE era stato chiesto di interpretare l'articolo 13, paragrafo 1, della direttiva 95/46. Questo articolo ha concesso agli Stati membri la scelta se adottare misure legislative intese a limitare la portata

del diritto dell’interessato di essere informato qualora necessario per proteggere, tra l’altro, i diritti e le libertà degli altri e per prevenire e indagare reati o violazioni della deontologia per le professioni regolamentate. L’IPI è un organismo professionale di agenti immobiliari in Belgio, responsabile di garantire il rispetto del buon esercizio della professione di agente immobiliare. Esso aveva chiesto a un giudice nazionale di dichiarare che i convenuti avevano violato norme professionali e di ordinare la cessazione di varie attività immobiliari. L’azione era basata su prove fornite da investigatori privati ai quali l’IPI era ricorsa.

Il giudice nazionale aveva espresso dubbi circa il valore delle prove fornite dagli investigatori, tenuto conto della possibilità che fossero state ottenute senza rispettare le prescrizioni in materia di tutela dei dati previste dal diritto belga, in particolare l’obbligo di informare gli interessati del trattamento dei loro dati personali prima della raccolta di tali informazioni. La CGUE ha rilevato che l’articolo 13, paragrafo 1, stabiliva che gli Stati membri «possono» prevedere nell’ordinamento nazionale deroghe all’obbligo di informare gli interessati in merito al trattamento dei loro dati, ma non ne hanno l’obbligo. Dal momento che l’articolo 13, paragrafo 1, include la prevenzione, la ricerca, l’accertamento e il perseguimento di infrazioni penali o violazioni della deontologia, sulla base

delle quali gli Stati membri possono limitare i diritti delle persone, un organismo come l'IPI e gli investigatori privati che agiscono a suo nome avrebbero potuto avvalersi di tale disposizione. Tuttavia, se uno Stato membro non ha previsto tale deroga, gli interessati devono essere informati.

Esempio: nella causa *Smaranda Bara e a. c. Casa Naţională de Asigurări de Sănătate e a.*[5 30], la CGUE ha chiarito se il diritto dell'UE osti a che un'amministrazione pubblica nazionale trasmetta dati personali a un'altra amministrazione pubblica a fini di trattamento successivo, senza che gli interessati siano informati né di tale trasmissione né del successivo trattamento. Nel caso di specie, l'agenzia nazionale per l'amministrazione tributaria non aveva informato i ricorrenti della trasmissione dei loro dati alla cassa nazionale malattia, prima della trasmissione stessa.

La CGUE ha stabilito che l'obbligo previsto dal diritto dell'UE di informare gli interessati del trattamento dei loro dati personali è «ancora più rilevante

poiché condiziona necessariamente l'esercizio da parte loro dei diritti, da un lato, di accesso ai dati trattati e della rispettiva rettifica, [...] e, dall'altro, di opposizione al trattamento dei medesimi». Il principio di trattamento leale obbliga a informare gli interessati della trasmissione dei loro dati a un'altra amministrazione pubblica, che li tratterà ulteriormente. Ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46, gli Stati membri possono limitare il diritto di essere informati qualora lo si ritenga necessario alla salvaguardia di un rilevante interesse economico dello Stato, comprese le questioni tributarie. Tuttavia, tali restrizioni devono essere adottate a mezzo di legge. Dal momento che né la definizione delle informazioni trasmissibili né le modalità dettagliate di attuazione della trasmissione, erano state previste in una misura legislativa, ma unicamente nel protocollo stipulato tra le due autorità pubbliche, le condizioni di deroga previste dal diritto dell'UE non erano soddisfatte. I ricorrenti avrebbero dovuto essere previamente informati della trasmissione dei loro dati alla cassa nazionale malattia e del loro successivo trattamento da parte dell'organismo.

Contenuto delle informazioni

Ai sensi dell'articolo 8, paragrafo 1, della Convenzione n. 108 modernizzata, il titolare del trattamento è tenuto a fornire all'interessato tutte le

informazioni necessarie per garantire un trattamento equo e trasparente dei dati personali, compresi:

- l'identità del titolare del trattamento e la sua sede legale;

- la base giuridica e le finalità del trattamento previsto;

- le categorie dei dati personali trattati;

- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

- le modalità con cui gli interessati possono esercitare i loro diritti.

Ai sensi del RGPD, in caso di raccolta di dati personali presso l'interessato, il titolare del trattamento è tenuto a fornire allo stesso, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni[531]:

- l’identità e i dati di contatto del titolare del trattamento compresi, ove applicabile, quelli del suo RPD;

- le finalità e la base giuridica del trattamento, ad esempio, un contratto o un obbligo legale;

- i legittimi interessi del titolare del trattamento, qualora costituiscano la base dello stesso;

- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

- l’eventualità che i dati siano trasferiti a un paese terzo o a un’organizzazione internazionale, e se questo si fondi su una decisione di adeguatezza o goda di garanzie appropriate;

- il periodo di conservazione dei dati personali e, se la determinazione di tale periodo non è possibile, i criteri utilizzati per determinare tale periodo di conservazione;

- i diritti dell’interessato riguardanti il trattamento, quali i diritti di accesso, ret- tifica, cancellazione e limitazione o opposizione in relazione al trattamento;

- se la comunicazione di dati personali è prevista per legge o da contratto, se l’interessato ha l’obbligo

di fornire i propri dati personali nonché le conseg-uenze della mancata comunicazione degli stessi;

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione;

- il diritto di proporre reclamo a un'autorità di controllo;

- l'esistenza del diritto di revocare il consenso.

Nel caso di processi decisionali automatizzati, compresa la profilazione, gli interessati devono ricevere informazioni significative sulla logica utilizzata nella profilazione nonché sulla sua importanza e sulle conseguenze previste di tale trattamento.

Nei casi in cui i dati personali non sono ottenuti direttamente dall'interessato, il titolare del trattamento deve notificare alla persona l'origine dei dati personali.

In ogni caso, il titolare del trattamento è tenuto, tra l'altro, a informare gli inter- essati dell'esistenza di processi decisionali automatizzati, compresa la profilazi- one[532]. Infine, qualora un titolare del trattamento intenda trattare dati personali per una finalità diversa da quella originariamente dichiarata all'interessato, il principio di limitazione della finalità e il principio di trasparenza prevedono che il titolare del trattamento fornisca all'interessato informazioni in merito a tale nuova finalità. I titolari del trattamento devono fornire le informazioni prima di qualsiasi ulteriore trattamento. In altri termini, nei casi in cui l'interessato abbia fornito il consenso al trattamento dei dati personali, il titolare del trattamento deve ottenere un rinnovo del consenso dell'interessato, se la finalità del tratta- mento è cambiata o se vengono aggiunte ulteriori finalità.

Tempistiche per la fornitura delle informazioni

Il RGPD distingue due scenari e due momenti in cui il titolare del trattamento dei dati deve fornire informazioni all'interessato.

- In caso di raccolta di dati personali direttamente presso l'interessato, il tito- lare del trattamento deve comunicare a quest'ultimo, nel momento in cui i dati sono ottenuti, tutte le informazioni e i diritti che lo riguardano ai sensi del RGPD[533].

Qualora intenda trattare ulteriormente i dati personali per una finalità diversa, il titolare del trattamento deve fornire, prima di effettuare tale trattamento, tutte le informazioni pertinenti.

- Qualora i dati personali non siano stati ottenuti direttamente presso l'interessato, il titolare del trattamento è tenuto a fornire a quest'ultimo informazioni concernenti il trattamento «entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese», o prima che i dati siano comunicati a terzi[534].

La relazione esplicativa della Convenzione n. 108 modernizzata prevede che qualora non sia possibile informare gli interessati all'inizio del trattamento, ciò può essere effettuato in un momento successivo, ad esempio, quando il titolare del trattamento viene messo in contatto con l'interessato per una ragione qualsiasi[535].

Diverse modalità di fornitura delle informazioni

Nell'ambito del diritto sia dell'UE sia del CdE, le informazioni che il titolare del trat- tamento deve fornire agli interessati devono essere concise, trasparenti, compren- sibili e facilmente accessibili. Devono essere fornite per iscritto o con altri mezzi, compresi i mezzi elettronici, utilizzando un linguaggio chiaro, semplice e facil- mente comprensibile. Nel fornire le informazioni, il titolare del trattamento può utilizzare icone standardizzate per fornire le informazioni in modo facilmente visi- bile e leggibile[536]. Ad esempio, un'icona che rappresenta un lucchetto può essere utilizzata per indicare che i dati sono raccolti e/o cifrati in modo sicuro. Gli interes- sati possono chiedere che le informazioni siano fornite oralmente. Le informazioni devono essere gratuite, a meno che le richieste dell'interessato siano manifesta- mente infondate o eccessive (ad esempio, di natura ripetitiva)[537]. Un facile accesso alle informazioni fornite è fondamentale affinché l'interessato possa esercitare i diritti che gli sono

conferiti dal diritto dell'UE in materia di protezione dei dati.

Il principio di correttezza del trattamento esige che le informazioni siano facil- mente comprensibili agli interessati. Il linguaggio adoperato deve essere appro- priato per i destinatari. Il livello e il tipo di linguaggio utilizzato devono differen- ziarsi in funzione del pubblico di riferimento, per esempio un adulto o un minore, pubblico in generale o un esperto accademico. La questione delle modalità per bilanciare questo aspetto della comprensibilità delle informazioni è trattata nel parere del Gruppo di lavoro articolo 29 sulla maggiore armonizzazione della for- nitura di informazioni. Ciò promuove l'idea delle cosiddette avvertenze multi- strato[538], che consentono all'interessato di decidere in merito al livello di dettag- lio delle informazioni. Nondimeno, questa modalità di presentare le informazioni

non solleva il titolare del trattamento dall'obbligo che gli incombe ai sensi degli articoli 13 e 14 del RGPD. Il titolare del trattamento deve comunque fornire tutte le informazioni all'interessato.

Uno dei modi più efficaci per fornire le informazioni è quello di prevedere ade- guate clausole informative sulla pagina iniziale del sito Internet del titolare del trattamento, come per esempio una politica sulla riservatezza relativa al sito Internet. Vi è tuttavia una parte considerevole della popolazione che non utilizza Internet e la politica d'informazione di una società o di un'autorità pubblica deve tenere conto di questo aspetto.

Un'informativa sulla privacy relativa al trattamento dei dati personali in una pagina web potrebbe presentarsi come segue:

Chi siamo?

«Titolare» del trattamento dei dati è Bed and Breakfast C&U, con sede in [indirizzo: xxx], tel: xxx; fax: xxx; e-mail: info@c&u.com; dati di contatto del responsabile della protezione dei dati: [xxx].

L'informativa sui dati personali fa parte dei termini e delle condizioni che regolano i nostri servizi alberghieri.

Quali dati personali raccogliamo?

Raccogliamo i seguenti dati personali dell'utente: nome, indirizzo postale, numero di telefono, indirizzo email, informazioni sul soggiorno, numero di carta di credito e carta di debito e indirizzi IP o nomi di dominio dei computer utilizzati per collegarsi al nostro sito Internet.

Perché raccogliamo i dati personali degli utenti?

Trattiamo i dati sulla base del consenso dell'utente e con la finalità di effettuare prenotazioni, concludere e dare esecuzione ai contratti relativi ai servizi da noi offerti e rispettare le prescrizioni di legge, ad esempio, la legge sull'imposta locale, che ci richiede di raccogliere i dati personali per rendere possibile il pagamento della tassa comunale di soggiorno.

Come trattiamo i dati degli utenti?

I dati personali dell'utente saranno conservati per un periodo di tre mesi e non sono soggetti a procedure decisionali automatizzate.

Bed and Breakfast C&U segue rigorose procedure di sicurezza al fine di garantire che le informazioni personali fornite dall'utente non siano danneggiate, distrutte o divulgate a terzi senza il consenso dello stesso, e per impedire l'accesso non autorizzato. I computer in cui sono archiviate le informazioni sono conservati in un ambiente sicuro, con accesso fisico limitato. Utilizziamo firewall sicuri e altre misure per limitare l'accesso elettronico. Qualora i dati debbano essere trasferiti a terzi, poniamo in essere misure analoghe, al fine di proteggere i dati personali dell'utente.

Tutte le informazioni raccolte o registrate sono riservate ai nostri uffici. Solo le persone che necessitano delle informazioni per adempiere alle loro funzioni ai sensi del presente contratto hanno accesso ai dati personali. Eventuali informazioni necessarie all'identificazione dell'utente saranno oggetto di richiesta esplicita. La cooperazione dell'utente con i nostri controlli di sicurezza può essere necessaria prima della comunicazione di informazioni allo stesso. L'utente può aggiornare in qualsiasi momento le

informazioni personali che ci ha fornito, contattandoci direttamente.

Quali sono i diritti dell'utente?

L'utente ha il diritto di accedere ai propri dati, ottenere copia degli stessi, chiedere la loro cancellazione o rettifica, o chiedere che i dati siano trasferiti a un altro titolare del trattamento.

Eventuali richieste possono essere comunicate all'indirizzo info@c&u.com. La risposta alle richieste sarà fornita entro un mese; tuttavia, se la richiesta è troppo complessa o in caso di troppe richieste, informeremo l'utente che tale periodo potrà essere prorogato di altri due mesi.

Accesso ai dati personali

L'utente ha il diritto di accedere ai propri dati e di essere messo a conoscenza, su richiesta, delle ragioni alla base del trattamento degli stessi, di chiederne

la cancellazione o la rettifica e di non essere oggetto di una decisione puramente automatizzata, che non tenga conto della sua opinione. Eventuali richieste possono essere comunicate all'indirizzo info@c&u.com. L'utente ha altresì il diritto di opporsi al trattamento, di revocare il proprio consenso e di presentare un reclamo presso l'autorità nazionale di controllo qualora ritenga che il presente trattamento sia in violazione della legge e di chiedere il risarcimento dei danni subiti a seguito del trattamento illecito.

Diritto di proporre reclamo

Il RGPD stabilisce che il titolare del trattamento deve informare gli interessati in merito a meccanismi di contrasto previsti dal diritto nazionale e dell'UE per i casi di violazione dei dati personali. Il titolare del trattamento deve informare gli interessati circa il loro diritto di presentare un reclamo a un'autorità di con- trollo e, se necessario, dinanzi a un giudice nazionale, in merito a una violazi- one dei dati personali[539]. Le disposizioni del Consiglio d'Europa sanciscono il diritto dei titolari dei dati a essere informati sui mezzi a loro disposizione per esercitare i loro diritti, incluso il diritto di rettifica previsto dall'articolo 9(1) (f).

Deroghe all'obbligo d'informazione

Il RGPD prevede una deroga all'obbligo di informare. Ai sensi dell'articolo 13, paragrafo 4, e dell'articolo 14, paragrafo 5, del RGPD, l'obbligo di informare gli interessati non si applica se l'interessato dispone già di tutte le informazioni per- tinenti[540]. Inoltre, qualora i dati personali non siano stati ottenuti dall'interessato, l'obbligo di informare non si applica se comunicare le informazioni risulta impossi- bile o sproporzionato, in particolare se i dati personali sono trattati a fini di archiv- iazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[541].

Inoltre, gli Stati membri dispongono di un margine di discrezionalità nell'ambito del RGPD, per limitare gli obblighi e i diritti delle persone ai sensi del regola- mento, qualora si tratti di una misura necessaria e proporzionata in una società democratica, per esempio, per la salvaguardia della sicurezza nazionale e pub- blica, della difesa, di indagini e procedimenti giudiziari, o per tutelare interessi

economici e finanziari, nonché interessi privati quando prevalgono sugli interessi della protezione dei dati[542].

Qualsiasi esenzione o limitazione deve essere necessaria in una società demo- cratica e proporzionata allo scopo perseguito. In casi del tutto eccezionali, per esempio a causa di prescrizioni mediche, la tutela dell'interessato può esigere di per sé una limitazione della trasparenza connessa, in particolare, alla limitazione del diritto di accesso degli interessati[543]. Come livello minimo di protezione, tutta- via, la legge nazionale deve rispettare il contenuto essenziale dei diritti e delle lib- ertà fondamentali tutelati dal diritto dell'UE[544]. Ciò presuppone che il diritto nazi- onale contenga disposizioni specifiche, che chiariscano le finalità del trattamento, comprese le categorie di dati personali, garanzie e altri obblighi procedurali[545].

Se i dati sono raccolti a fini di ricerca scientifica o storica, a fini statistici o di archiviazione nel pubblico interesse, l'Unione o gli Stati membri possono preve- dere deroghe all'obbligo di informare, se rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche[546].

Simili limitazioni sono applicabili dinanzi alle disposizioni del Consiglio d'Europa, laddove i diritti garantiti ai titolari dei dati dall'articolo 9 della

Convenzione modernizzata possono andare incontro a restrizioni dinanzi all'articolo 11 della Convenzione modernizzata 108, a condizioni rigorose. In aggiunta, in conform- ità all'articolo 8(2) della Convenzione modernizzata l'obbligo alla trasparenza imposto ai controllori non è applicabile nel caso in cui il soggetto titolare dei dati sia già in possesso delle informazioni.

Diritto di accesso ai propri dati

Ai sensi del diritto del CdE, il diritto di accesso ai propri dati è riconosciuto esplicitamente all’articolo 9 della Convenzione n. 108 modernizzata. Esso pre- vede che ogni persona abbia il diritto di ottenere, su richiesta, informazioni circa il trattamento dei dati personali che la riguardano, comunicate in forma intelligibile. Il diritto di accesso è stato riconosciuto non solo nelle disposizioni della Convenzione n. 108 modernizzata, ma anche nella giurisprudenza della Corte EDU. La Corte EDU ha affermato a più riprese il diritto di accesso delle

persone alle informazioni relative ai loro dati personali, ribadendo il fatto che tale diritto sorge dalla necessità di rispettare la vita privata[547]. Tuttavia, il diritto di accesso ai dati personali archiviati da organizzazioni pubbliche o private può essere limitato in alcune circostanze[548].

Nell'ambito del diritto dell'UE, il diritto di accesso ai propri dati è esplicita- mente riconosciuto dall'articolo 15 del RGPD ed è inoltre sancito come parte del diritto fondamentale alla protezione dei dati personali nell'articolo 8, para- grafo 2, della Carta dei diritti fondamentali dell'UE[549]. Il diritto di una persona di accedere ai propri dati personali è un elemento fondamentale della normativa europea in materia di protezione dei dati[550].

Il RGPD stabilisce che ogni interessato ha il diritto di ottenere dal titolare del trattamento l'accesso ai dati personali e a talune informazioni riguardanti il trat- tamento[551]. In particolare, ogni interessato ha il diritto di ottenere (dal titolare del trattamento) la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e l'accesso almeno alle seguenti informazioni:

- finalità del trattamento;
- categorie di dati in questione;

- destinatari o categorie di destinatari a cui i dati sono comunicati;

- periodo di conservazione dei dati personali previsto oppure, se non è pos- sibile, criteri utilizzati per determinare tale periodo;

- esistenza del diritto di rettificare o cancellare i dati personali o limitare il loro trattamento;

- diritto di proporre reclamo all'autorità di controllo;

- tutte le informazioni disponibili sull'origine dei dati oggetto del trattamento, qualora i dati non siano raccolti presso l'interessato;

- nel caso di decisioni automatizzate, la logica applicata nei trattamenti automatiz- zati dei dati.

Il titolare del trattamento deve fornire all'interessato una copia dei dati personali oggetto di trattamento. Tutte le informazioni comunicate all'interessato devono essere fornite in forma intelligibile, vale a dire che il titolare del trattamento deve assicurarsi che l'interessato possa capire le informazioni fornite. Ad esempio, inclu- dere abbreviazioni tecniche, termini codificati o acronimi in risposta a una richiesta di accesso, non sarà in genere sufficiente, a meno che non venga spiegato il sig- nificato di tali termini. In caso di processi decisionali automatizzati, compresa la profilazione, occorre illustrare la logica generale del processo decisionale automa- tizzato, compresi i criteri specifici presi in considerazione in sede di valutazione dell'interessato. Requisiti analoghi sono previsti ai sensi del diritto del CdE[552]

Esempio: l'accesso ai propri dati personali aiuterà l'interessato a determinare la correttezza o meno dei dati. È pertanto essenziale che l'interessato sia

informato, in forma intelligibile, non solo dei dati personali effettivamente trattati, ma anche delle categorie in cui tali dati personali sono trattati, quali nome, indirizzo IP, coordinate di geolocalizzazione, numero di carta di credito, ecc.

Quando i dati non sono ottenuti dall'interessato, l'informazione sull'origine degli stessi deve essere fornita in risposta a una richiesta di accesso nella mis- ura in cui tale informazione è disponibile. Detta disposizione deve essere intesa nel quadro dei principi di correttezza, di trasparenza e di responsabilizzazione. Un titolare del trattamento non può eliminare le informazioni sull'origine dei dati per essere dispensato dal divulgarle, a meno che l'eliminazione avrebbe avuto luogo nonostante il ricevimento della richiesta di accesso, e deve comunque rispettare i requisiti generali in materia di «responsabilizzazione».

Come rilevato nella giurisprudenza della CGUE, il diritto di accesso ai dati personali non deve essere indebitamente ristretto da limiti temporali. Gli

interessati devono inoltre avere una ragionevole possibilità di acquisire informazioni sulle operazioni di trattamento dei dati effettuate in passato.

Esempio: nella causa *Rijkeboer*[553], la CGUE è stata chiamata a determinare se il diritto di una persona di accedere alle informazioni sui destinatari o sulle categorie di destinatari dei dati personali e al contenuto dei dati potesse essere limitato a un anno prima della sua richiesta di accesso.

Al fine di stabilire se la legislazione dell'UE autorizzi una siffatta limitazione temporale, la CGUE ha deciso di interpretare l'articolo 12 alla luce degli obiettivi della direttiva. La CGUE ha dichiarato in primo luogo che il diritto di accesso è necessario affinché l'interessato possa esercitare il diritto di ottenere dal titolare del trattamento la rettifica, la cancellazione o il blocco del trattamento dei suoi dati o affinché egli notifichi tale rettifica, cancellazione o blocco ai terzi cui sono stati comunicati tali dati. Un diritto effettivo di accesso è anche necessario per consentire all'interessato l'esercizio del diritto di opposizione al trattamento dei suoi dati personali o il diritto di presentare un reclamo e chiedere il risarcimento dei danni[554].

Per garantire l'effetto utile dei diritti conferiti agli interessati, la CGUE ha statuito che «tale diritto deve necessariamente estendersi al passato. In caso

contrario, infatti, la persona interessata non sarebbe in grado di esercitare efficacemente il suo diritto a fare rettificare, cancellare o congelare i dati ritenuti illeciti o non corretti nonché a procedere giurisdizionalmente ed ottenere il risarcimento del pregiudizio subito».

6.1.2. Diritto di rettifica

Nell’ambito del diritto dell’UE e del CdE, gli interessati hanno il diritto di ottenere la rettifica dei propri dati personali. L’esattezza dei dati personali è fondamentale per garantire un elevato livello di protezione dei dati per gli interessati[555].

Esempio: nella causa *Ciubotaru c. Moldova*[556], il ricorrente non aveva potuto modificare l'indicazione della propria origine etnica, contenuta nei registri ufficiali, da moldava a rumena, asseritamente a causa del fatto che non era riuscito a suffragare tale richiesta. La Corte EDU ha ritenuto accettabile che gli Stati richiedessero prove oggettive all'atto della registrazione dell'identità etnica di una persona. Quando tali richieste sono basate su motivi puramente soggettivi e non comprovati, le autorità potrebbero respingerle. Tuttavia, la richiesta del ricorrente si fondava su qualcosa di più di una mera percezione soggettiva della propria etnia: egli era stato in grado di dimostrare legami oggettivamente verificabili con il gruppo etnico rumeno quali la lingua, il nome, l'affinità ecc. Tuttavia, secondo il diritto nazionale, il ricorrente era obbligato a dimostrare che i suoi genitori erano appartenuti al gruppo etnico rumeno. Date le realtà storiche della Moldova, tale requisito aveva creato un ostacolo insormontabile alla registrazione di un'identità etnica diversa da quella registrata per i suoi genitori dalle autorità sovietiche. Impedendo al ricorrente di fare esaminare la sua domanda alla luce di prove oggettivamente verificabili, lo Stato non aveva ottemperato all'obbligo positivo di garantire al ricorrente l'effettivo rispetto della sua vita privata. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

In alcuni casi basterà semplicemente che l'interessato chieda la rettifica, per esempio, della grafia di un nome oppure il cambio di un indirizzo o di un numero di telefono. Nell'ambito del diritto dell'UE e del diritto del CdE, i dati personali inesatti devono essere rettificati senza ingiustificato o eccessivo ritardo[557]. Tuttavia, se tali richieste sono correlate a questioni giuridicamente rilevanti, come l'identità giuridica dell'interessato o l'esatto luogo di residenza per il rilascio di documenti legali, le richieste di rettifica possono rivelarsi insuf- ficienti e il titolare del trattamento può richiedere la prova della presunta ine- sattezza. Tali domande non devono imporre un irragionevole onere della prova sull'interessato, impedendogli così di ottenere la rettifica dei propri dati. La Corte EDU ha rilevato violazioni dell'articolo 8 della CEDU in diversi casi in cui il ricorrente non era stato in grado di contestare l'esattezza delle informazioni contenute in registri segreti[558].

Esempio: nella causa *Cemalettin Canli c. Turchia*[559], la Corte EDU ha constatato una violazione dell'articolo 8 della CEDU derivante dalla presentazione di un rapporto di polizia inesatto nel corso di un procedimento penale.

Il ricorrente era stato sottoposto a due procedimenti penali a causa della presunta appartenenza a organizzazioni illegali, ma non era stato condannato. Quando il ricorrente era stato nuovamente arrestato e accusato di un altro reato penale, la polizia aveva trasmesso al tribunale penale un rapporto intitolato «*modulo informativo su ulteriori reati*» nel quale si asseriva che il ricorrente era membro di due organizzazioni illegali. La richiesta del ricorrente concernente la modifica del rapporto e degli schedari della polizia era stata respinta. La Corte EDU ha ritenuto che le informazioni contenute nel rapporto di polizia rientrassero nell'ambito di applicazione dell'articolo 8 della CEDU, in quanto anche le informazioni pubbliche sistematicamente raccolte e conservate in fascicoli dalle autorità potevano rientrare nella nozione di «vita privata». Inoltre, il rapporto di polizia era inesatto e la sua formulazione e trasmissione al tribunale penale non erano conformi alla legislazione nazionale. La Corte EDU ha concluso asserendo la sussistenza di una violazione dell'articolo 8.

Nel corso di una causa civile o di un procedimento dinanzi a un’autorità pub- blica per stabilire l’esat tez za o meno dei dati, l’interessato può chiedere l’inserimento di una voce o di una nota nel proprio fascicolo attestante la con- testazione dell’esattezza dell’informazione inserita e l’attesa di una decisione ufficiale[560]. Durante questo periodo il titolare del trattamento non deve presen- tare i dati come corretti o soggetti a modifica, in particolare a terzi.

6.1.3. Diritto alla cancellazione («diritto all’oblio»)

Garantire agli interessati il diritto alla cancellazione dei propri dati è partico- larmente importante ai fini dell’efficace applicazione dei principi di protezione dei dati, segnatamente il principio di minimizzazione dei dati (i dati personali devono essere limitati a quanto necessario alle finalità per le quali vengono trattati). Il diritto alla cancellazione è pertanto previsto negli strumenti legali sia del CdE sia dell’UE[561].

Esempio: nella causa *Segerstedt-Wiberg e a. c. Svezia*[562], i ricorrenti erano stati membri di alcuni partiti politici di matrice liberale e comunista. Essi sospettavano che nei registri dei servizi segreti fossero state inserite informazioni sul loro conto e ne avevano chiesto la cancellazione. La Corte EDU ha stimato che la conservazione dei dati in questione avesse una base giuridica e perseguisse uno scopo legittimo. Tuttavia, per quanto riguarda alcuni ricorrenti, la Corte EDU ha dichiarato che la persistente conservazione dei dati costituiva un'ingerenza sproporzionata nelle loro vite private. Ad esempio, nel caso di uno dei ricorrenti, le autorità avevano conservato informazioni secondo le quali nel 1969 egli aveva asseritamente invocato la resistenza violenta contro i controlli di polizia nel corso di manifestazioni. La Corte EDU ha rilevato che detta informazione non avrebbe potuto perseguire alcun interesse rilevante di sicurezza nazionale, in particolare data la sua natura storica. La Corte ha riscontrato una violazione dell'articolo 8 della CEDU per quattro ricorrenti su cinque poiché, considerato il lungo lasso di tempo trascorso dai fatti attribuiti ai ricorrenti, la conservazione dei loro dati non aveva rilevanza.

Esempio: nella causa *Brunet c. Francia*[563], i ricorrenti avevano denunciato la conservazione dei loro dati personali in una banca dati della polizia, che conteneva informazioni concernenti condannati, imputati e vittime. I dettagli concernenti il ricorrente apparivano nella banca

dati, anche se il procedimento penale a carico dello stesso era stato archiviato. La Corte ha statuito che vi era stata una violazione dell'articolo 8 della CEDU. Nel giungere alla sua conclusione, la Corte ha ritenuto che, in pratica, il ricorrente non aveva alcuna possibilità di ottenere la cancellazione dei propri dati personali dalla banca dati. La Corte EDU ha preso in considerazione anche la natura delle informazioni contenute nella banca dati, ritenendola invasiva per la vita privata del ricorrente, dal momento che conteneva particolari della sua identità e della sua personalità. Inoltre, essa ha ritenuto che il periodo di conservazione dei fascicoli personali nella banca dati, della durata di 20 anni, fosse eccessivamente lungo, tanto più che nessun tribunale aveva mai condannato il ricorrente.

La Convenzione n. 108 modernizzata riconosce esplicitamente che tutte le per- sone hanno il diritto alla cancellazione dei dati personali inesatti, falsi o trattati illecitamente[564].

Nell'ambito del diritto dell'UE, l'articolo 17 del RGPD dà seguito alle richieste degli interessati di ottenere la cancellazione dei dati. Il diritto a ottenere la cancellazione dei propri dati personali senza ingiustificato ritardo si applica quando:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

- l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;

- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

- i dati personali sono stati trattati illecitamente;

- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il tito- lare del trattamento;

- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a minori, ai sensi dell'articolo 8 del RGPD[565].

L'onere della prova relativo alla legittimità del trattamento dei dati incombe sui titolari del trattamento, poiché questi sono responsabili della liceità dello stesso[566]. In base al principio di responsabilizzazione, il titolare del trattamento deve essere in grado di dimostrare in qualsiasi momento l'esistenza di una sol- ida base giuridica per il trattamento dei dati, diversamente il trattamento deve essere interrotto[567]. Il RGPD definisce le eccezioni al diritto all'oblio, compresi i casi in cui il trattamento dei dati personali è necessario per:

- l'esercizio del diritto alla libertà di espressione e di informazione;

- l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del tratta- mento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

- motivi di interesse pubblico nel settore della sanità pubblica;

- fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici;

- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria[568].

La CGUE ha affermato l'importanza del diritto alla cancellazione per garantire un livello elevato di protezione dei dati.

Esempio: nella causa *Google Spain*[569], la CGUE è stata chiamata a decidere se Google fosse tenuta ad eliminare dal suo elenco di risultati di ricerca le informazioni obsolete concernenti le difficoltà finanziarie del ricorrente. Google contestava, tra l'altro, la responsabilità che le veniva attribuita, sostenendo di limitarsi a fornire un collegamento ipertestuale alla pagina web dell'editore che ospita l'informazione, nel caso specifico, un quotidiano che riferiva di questioni attinenti all'insolvenza del ricorrente[570]. Google aveva sostenuto che la richiesta di eliminare informazioni obsolete da una pagina web dovrebbe essere presentata all'ospite della pagina web e non a Google, che si limita a fornire un link verso la pagina d'origine. La CGUE ha concluso che Google, quando cerca informazioni e pagine web in Internet e quando indicizza il contenuto per fornire i risultati

della ricerca, diventa un titolare del trattamento al quale si applicano responsabilità e obblighi ai sensi del diritto dell’UE.

La CGUE ha chiarito che i motori di ricerca su Internet e i risultati di ricerca che forniscono dati personali possono stabilire un profilo dettagliato di una persona[571]. I motori di ricerca rendono onnipresenti le informazioni contenute in un tale elenco di risultati. Alla luce della sua potenziale gravità,

tale ingerenza non può essere giustificata dal mero interesse economico dell'operatore di un siffatto motore di ricerca in tale trattamento di dati. In particolare, occorre ricercare un giusto equilibrio tra il legittimo interesse degli utenti di Internet nell'accesso all'informazione e i diritti fondamentali dell'interessato ai sensi degli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE. In una società sempre più digitalizzata, l'esigenza che i dati personali siano esatti e che il loro uso sia limitato alla loro necessità (ad esempio per le informazioni pubbliche) è fondamentale per garantire un livello elevato di protezione dei dati alle persone. Il «responsabile del trattamento in questione deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che tale trattamento soddisfi le prescrizioni» del diritto dell'UE, affinché le garanzie giuridiche previste sviluppino pienamente i loro effetti[572]. Ciò significa che il diritto di ottenere la cancellazione dei propri dati personali quando il trattamento è obsoleto o non più necessario, riguarda anche i titolari del trattamento che riproducono le informazioni[573].

Nell'esaminare se Google fosse tenuta o meno a eliminare i link collegati al ricorrente, la CGUE ha stabilito che, in determinate condizioni, le persone hanno il diritto di chiedere la cancellazione dei dati personali. Questo diritto può essere invocato qualora le informazioni relative a una persona

siano inesatte, inadeguate, non pertinenti o eccessive in rapporto alla finalità del trattamento. La CGUE ha riconosciuto che questo diritto non è assoluto; esso deve essere ponderato con altri diritti e interessi, in particolare l'interesse del grande pubblico ad avere accesso a determinate informazioni. Ogni richiesta di cancellazione deve essere valutata caso per caso, per trovare un equilibrio tra i diritti fondamentali alla protezione dei dati personali e della vita privata dell'interessato, da un lato, e gli interessi legittimi di tutti gli utenti di Internet, compresi gli editori, dall'altro. La CGUE ha fornito indicazioni sui fattori da considerare nello svolgimento di questa ponderazione. La natura dell'informazione di cui trattasi è un fattore particolarmente importante. Se l'informazione si riferisce alla vita privata della persona

e non vi è interesse pubblico alla sua disponibilità, la protezione dei dati e della vita privata prevarrebbe sul diritto del pubblico generale di avere accesso all'informazione. Al contrario, ove risulti che l'interessato è una figura pubblica o che l'informazione è di natura tale da giustificarne l'accessibilità al pubblico, l'interesse preponderante del grande pubblico ad avere accesso all'informazione potrebbe giustificare l'ingerenza nei diritti fondamentali alla protezione dei dati e alla vita privata dell'interessato.

A seguito della sentenza, il Gruppo di lavoro articolo 29 ha adottato linee guida per l'attuazione della sentenza della Corte di giustizia[574]. Le linee guida com- prendono un elenco di criteri comuni che le autorità di controllo devono utiliz- zare nella gestione dei reclami relativi alle richieste di cancellazione da parte di persone fisiche, nelle quali vengono illustrate le conseguenze di tale diritto alla cancellazione e forniscono un orientamento per la ponderazione dei diritti. Le linee guida ribadiscono che le valutazioni devono essere effettuate caso per caso. Dal momento che il diritto all'oblio non è assoluto, il risultato di una richi- esta può variare a seconda del caso in questione. Ciò è illustrato anche nella giurisprudenza della CGUE dopo Google.

Esempio: nella causa *Camera di Commercio di Lecce c. Manni*[575], la CGUE doveva esaminare se una persona avesse il diritto di ottenere la cancellazione dei suoi dati personali iscritti in un pubblico registro delle imprese, dopo che la sua società aveva cessato di esistere. Il sig. Manni aveva chiesto alla Camera di commercio di Lecce di cancellare i suoi dati personali da tale registro, avendo scoperto che i potenziali clienti, consultando il registro, avrebbero visto che in precedenza egli era stato amministratore di una società dichiarata fallita più di un decennio prima. Il ricorrente riteneva che questa informazione avrebbe dissuaso i potenziali clienti.

Nel ponderare il diritto del sig. Manni alla protezione dei suoi dati personali con l'interesse del pubblico generale ad accedere alle informazioni, la CGUE ha innanzitutto esaminato la finalità del pubblico registro. Essa ha sottolineato

il fatto che la pubblicità era prevista per legge e, segnatamente, da una direttiva dell'UE volta a facilitare l'accesso di terzi alle informazioni sulle società. I terzi devono pertanto avere accesso ed essere in grado di esaminare gli atti essenziali di una società e altre indicazioni che la concernono, «in particolare le generalità delle persone che hanno il potere di obbligarla». Scopo della pubblicità era anche garantire la certezza del diritto in previsione di un incremento degli scambi commerciali fra gli Stati membri, garantendo ai terzi l'accesso a tutti i dati pertinenti in tutta l'UE.

La CGUE ha inoltre osservato che anche dopo il decorso del tempo, e perfino dopo lo scioglimento di una società, diritti e obblighi giuridici relativi alla stessa possono perdurare. Le controversie relative a una dissoluzione possono estendersi in un lungo arco di tempo e questioni concernenti la società, i suoi amministratori e liquidatori possono sorgere per molti anni dopo che la società ha cessato di esistere. La CGUE ha sostenuto che, alla luce della molteplicità dei possibili scenari e delle differenze dei termini di prescrizione previsti in ciascuno Stato membro, «allo stato attuale risulta impossibile identificare un termine univoco, a far data dallo scioglimento di una società, allo spirare del quale non sarebbe più necessaria l'iscrizione nel registro e la pubblicità dei dati citati». In ragione dello scopo legittimo della pubblicità e della difficoltà di determinare un periodo al termine del quale i dati

personali possono essere cancellati dal registro senza pregiudicare gli interessi di terzi, la CGUE ha ritenuto che le norme dell'UE in materia di protezione dei dati non garantiscono il diritto alla cancellazione dei dati personali per le persone nella situazione del sig. Manni.

Qualora il titolare del trattamento abbia reso pubblici i dati personali e sia tenuto a cancellare le informazioni, ha l'obbligo di farlo e deve adottare misure
«ragionevoli» per informare gli altri titolari del trattamento degli stessi dati, in merito alla richiesta di cancellazione avanzata dall'interessato. Le attività del titolare del trattamento devono tenere conto delle tecnologie disponibili e dei costi di attuazione[576]

6.1.4. Diritto di limitazione di trattamento

L'articolo 18 del RGPD autorizza gli interessati a ottenere dal titolare del trat- tamento la limitazione provvisoria del trattamento dei loro dati personali. Gli interessati possono chiedere al titolare la limitazione del trattamento quando:

- viene contestata l'esattezza dei dati personali;

- il trattamento è illecito e l'interessato chiede la limitazione dell'utilizzo dei dati personali invece della cancellazione;

- i dati devono essere conservati per l'esercizio o la difesa di un diritto in sede giudiziaria;

- è pendente una decisione in merito all'eventuale prevalenza dei motivi leg- ittimi del titolare del trattamento rispetto a quelli dell'interessato[577].

Le modalità con cui un titolare del trattamento può limitare il trattamento dei dati personali possono consistere, per esempio, nel trasferire temporanea- mente i dati selezionati verso un altro sistema di trattamento, rendere i dati inaccessibili agli utenti o rimuovere temporaneamente i dati personali[578]. Il tito- lare del trattamento deve informare l'interessato prima di revocare la limitazi- one al trattamento[579].

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento deve comunicare eventuali rettifiche o cancellazi- oni dei dati personali o limitazioni del trattamento a ciascuno dei destinatari cui sono stati trasmessi i dati personali, salvo che ciò si riveli impossibile o sproporzionato[580]. Se l'interessato richiede informazioni riguardanti tali desti- natari, il titolare del trattamento è tenuto a fornirgli tali informazioni[581].

6.1.5. Diritto alla portabilità dei dati

Ai sensi del RGPD, gli interessati hanno diritto alla portabilità dei dati in situ- azioni in cui i dati personali che hanno fornito a un titolare dei dati sono trattati con mezzi automatizzati sulla base del consenso o qualora il trattamento dei dati personali sia necessario per l'esecuzione di un contratto e i dati siano trat- tati con mezzi automatizzati. Questo significa che il diritto alla portabilità dei dati non si applica qualora il trattamento dei dati personali si basi su un fonda- mento giuridico diverso dal consenso o contratto[582].

Se il diritto alla portabilità dei dati è applicabile, gli interessati hanno il diritto di ottenere la trasmissione diretta dei loro dati personali da un titolare del tratta- mento all'altro, se tecnicamente fattibile[583]. A tal fine, il titolare del trattamento deve sviluppare formati interoperabili che consentano la portabilità dei dati[584]. Il RGPD precisa che tali formati devono essere strutturati, di uso comune e leg- gibili da dispositivo automatico per facilitare l'interoperabilità[585]. Quest'ultima può essere definita, in senso lato, come la capacità di sistemi di informazi- one di scambiare dati e di consentire la condivisione delle informazioni[586]. Pur essendo lo scopo dei formati utilizzati quello di garantire l'interoperabilità, il RGPD non impone raccomandazioni particolari circa il formato specifico

tras- messo: i formati possono differire a seconda del settore[587].

Secondo le linee guida del Gruppo di lavoro articolo 29, il diritto alla portabilità dei dati «mira a promuovere la libertà di scelta degli utenti, il loro controllo sui trattamenti e i loro diritti», con l'obiettivo di garantire agli interessati il con- trollo sui loro dati personali[588]. Le linee guida chiariscono i principali elementi della portabilità dei dati, che comprendono:

- il diritto degli interessati a ricevere i propri dati personali trattati dal titolare del trattamento in un formato strutturato, di uso comune, leggibile da dis- positivo automatico e interoperabile;

- il diritto di trasmettere i dati personali da un titolare del trattamento a un altro titolare del trattamento, senza impedimenti ove ciò sia tecnicamente possibile;

- la titolarità del trattamento: quando un titolare del trattamento dà seguito a una richiesta di portabilità, egli agisce per conto dell'interessato, nel senso che non è responsabile dell'osservanza delle norme in materia di protezi- one dei dati da parte del ricevente, visto che è l'interessato che decide a chi i dati vengono trasmessi;

- l'esercizio del diritto alla portabilità dei dati non pregiudica nessuno degli altri diritti; lo stesso è vero per tutti gli altri diritti riconosciuti dal RGPD.

6.1.6. Diritto di opposizione

Gli interessati possono far valere il loro diritto di opporsi al trattamento dei dati personali per motivi connessi alla loro situazione particolare e al trattamento dei dati per finalità di marketing diretto. Il diritto di opposizione può essere esercitato con mezzi automatizzati.

Diritto di opposizione per motivi connessi alla situazione particolare dell'interessato

Gli interessati non godono di un diritto generale di opporsi al trattamento dei propri dati[589]. L'articolo 21, paragrafo 1, del RGPD conferisce all'interessato il diritto di opporsi al trattamento che riguarda la sua situazione par ticolare quando la base giuridica dello stesso è l'esecuzione da parte del titolare del trattamento di un compito svolto nel pubblico interesse o quando il tratta- mento si basa sui legittimi interessi del titolare del trattamento[590]. Il diritto di opposizione si applica alle attività di profilazione. Un diritto analogo è stato riconosciuto nella Convenzione n. 108 modernizzata[591].

Il diritto di opporsi per motivi connessi alla situazione particolare dell'interessato mira a trovare il giusto equilibrio tra i diritti di protezione dei dati dell'interessato e i diritti legittimi di terzi nel trattamento di dati che li riguardano. La GCUE, tuttavia, ha precisato che i diritti dell'interessato prevalgono «di norma» sugli interessi economici di un titolare del trattamento e «dipendono dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione»[592]. Ai sensi del RGPD, l'onere della prova spetta ai titolari del trattamento, i quali devono dimostrare motivi preminenti per continuare il trat- tamento[593]. In modo analogo, la relazione esplicativa della Convenzione n. 108 modernizzata precisa che i motivi legittimi per il trattamento dei dati (che possono prevalere sul diritto di opporsi degli interessati) devono essere dimostrati caso per caso[594].

Esempio: nella causa *Manni*[595], la CGUE ha ritenuto che, in ragione della finalità legittima della pubblicità dei dati personali nel registro delle imprese, in particolare della necessità di proteggere gli interessi di terzi e garantire la certezza del diritto, in linea di principio, il sig. Manni non aveva il diritto di ottenere la cancellazione dei suoi dati personali dal registro delle imprese. Tuttavia, essa ha riconosciuto l'esistenza di un diritto di opporsi al trattamento,

dichiarando che «non si può [...] escludere che possano sussistere situazioni particolari in cui ragioni preminenti legittime connesse al caso concreto della persona interessata giustifichino, in via eccezionale, che l'accesso ai dati personali ad essa relativi iscritti nel registro sia limitato, decorso un periodo di tempo sufficientemente lungo [...] ai terzi che dimostrino un interesse specifico alla loro consultazione».

La CGUE ha ritenuto che spettasse ai giudici nazionali valutare ciascun caso, tenendo conto dell'insieme delle circostanze rilevanti dell'interessato e dell'eventuale esistenza di ragioni legittime e preminenti che potrebbero,

in via eccezionale, giustificare una limitazione all'accesso di terzi ai dati personali contenuti nei registri delle imprese. Nondimeno, essa ha precisato che, nel caso del sig. Manni, il solo presumere che la pubblicazione dei suoi dati personali nel registro influisse sulla sua clientela, non poteva essere sufficiente a costituire una simile ragione legittima e preminente. I potenziali clienti del sig. Manni avevano un interesse legittimo ad accedere alle informazioni concernenti il fallimento della sua precedente società.

L'effetto dell'accoglimento di un'opposizione è che il titolare del trattamento non può più trattare i dati in questione. Le operazioni di trattamento svolte sui dati dell'interessato prima dell'opposizione restano, tuttavia, legittime.

Diritto di opposizione all'ulteriore trattamento dei dati per finalità di marketing diretto

L'articolo 21, paragrafo 2, del RGPD prevede un diritto specifico di opporsi all'uso dei dati personali per finalità di marketing diretto, chiarendo ulteriormente l'articolo 13 della direttiva e-privacy. Un diritto analogo è sancito anche dalla Convenzione n. 108 modernizzata, nonché nella raccomandazione del CdE sul marketing diretto[596]. La relazione esplicativa della Convenzione n. 108 modernizzata

chiarisce che le obiezioni al trattamento dei dati per finalità di marketing diretto devono portare alla cancellazione o alla soppressione incondizionate dei dati personali di cui trattasi[597].

L'interessato ha il diritto di opporsi all'uso dei propri dati personali per final- ità di marketing diretto in qualsiasi momento e gratuitamente. Gli interessati devono essere informati di tale diritto chiaramente e separatamente da qual- siasi altra informazione.

Diritto di opposizione con mezzi automatizzati

Qualora dati personali siano utilizzati e trattati per servizi della società dell'informazione, l'interessato può esercitare il suo diritto di opporsi al trat- tamento dei propri dati personali con mezzi automatici.

I servizi della società dell'informazione sono definiti come qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi[598].

I titolari del trattamento che offrono servizi della società dell'informazione devono mettere in atto misure e procedure tecniche adeguate per garantire che il diritto di opposizione con mezzi automatizzati possa essere esercitato in modo efficace[599]. Ad esempio, bloccando i cookies nelle pagine web o disat- tivando la tracciatura della navigazione in Internet.

Diritto di obiezione per finalità di ricerca scientifica o storica o a fini statistici

Nell'ambito del diritto dell'UE, la ricerca scientifica dovrebbe essere interpre- tata in senso lato e includere, ad esempio, sviluppo tecnologico e dimostrazi- one, ricerca fondamentale, ricerca

applicata e ricerca finanziata da privati[600]. La ricerca storica comprende anche la ricerca a fini genealogici, tenendo conto del fatto che il regolamento non dovrebbe applicarsi ai dati delle persone dece- dute[601]. Per finalità statistiche si intende qualsiasi operazione di raccolta e trat- tamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici[602]. Ancora una volta, la situazione particolare di un interessato costituisce la base giuridica per il diritto di opporsi al trattamento dei dati per- sonali a fini di ricerca[603]. L'unica eccezione è costituita dalla necessità del trat- tamento ai fini dell'esecuzione di un compito di interesse pubblico. Tuttavia, il diritto alla cancellazione non si applica quando il trattamento è necessario (con

o senza motivi di interesse pubblico) a fini di ricerca scientifica o storica o a fini statistici[604].

Il RGPD concilia le esigenze della ricerca scientifica, statistica o storica e i diritti degli interessati con le garanzie e le deroghe specifiche di cui all'articolo 89. Pertanto, il diritto dell'Unione o dello Stato membro può prevedere deroghe al diritto di opporsi, nella misura in cui tale diritto rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca, e se tali deroghe sono necessarie al conseguimento di dette finalità.

Ai sensi del diritto del CdE, l'articolo 9, paragrafo 2, della Convenzione n. 108 modernizzata stabilisce che le limitazioni all'esercizio dei diritti degli interes- sati, compreso il diritto di obiezione, possono essere previste per legge per il trattamento dei dati a fini di archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici quando non esiste un rischio iden- tificabile di violazione dei diritti e delle libertà fondamentali degli interessati.

Tuttavia, la relazione esplicativa (punto 41) riconosce anche che gli interessati dovrebbero avere l'opportunità di prestare il proprio consenso solo per determi- nati settori di ricerca o parti di progetti di ricerca, nella misura consentita dalla finalità prevista, e di opporsi qualora percepiscano il trattamento come

eccessiva- mente pregiudizievole per i loro diritti e le loro libertà senza un motivo legittimo.

In altre parole, tale trattamento sarebbe quindi considerato a priori compati- bile, a condizione che esistano altre garanzie e che le operazioni escludano, in linea di principio, qualsiasi uso delle informazioni ottenute per decisioni o mis- ure riguardanti una persona in particolare.

6.1.7. Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

Le decisioni automatizzate sono decisioni adottate usando dati personali trat- tati esclusivamente con mezzi automatici, senza intervento umano.
Nell'ambito del diritto dell'UE, gli interessati non devono essere sottoposti a decisioni automatizzate che producano effetti giuridici o effetti significativi analoghi. Qualora sia probabile che tali decisioni abbiano un impatto significativo sulle

vite delle persone perché riguardano, ad esempio, l’affidabilità creditizia, le assunzioni elettroniche, il rendimento professionale o l’analisi del comportamento o l’affidabilità, è necessaria una protezione particolare per evitare con- seguenze negative. Tale processo decisionale automatizzato comprende la pro- filazione, che consiste in una forma di valutazione automatizzata degli «aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il com- portamento, l’ubicazione o gli spostamenti dell’interessato»[605].

Esempio: per accertare con rapidità l’affidabilità creditizia di un cliente futuro, le agenzie di valutazione del merito creditizio raccolgono taluni dati, quali le modalità con cui il cliente ha mantenuto i propri conti di credito e di servizi/ utenze, i dettagli sui precedenti indirizzi del cliente nonché informazioni da fonti pubbliche, come liste elettorali, registri pubblici (comprese le sentenze giudiziarie) o informazioni riguardanti fallimento o insolvenza. Questi dati personali sono successivamente inseriti in un algoritmo di valutazione, che calcola un valore generale rappresentativo dell’affidabilità creditizia del potenziale cliente.

Secondo il Gruppo di lavoro articolo 29, il diritto di non essere assoggettati a decisioni basate esclusivamente sul trattamento automatizzato, che potreb- bero comportare effetti giuridici per l'interessato o che incidono significativa- mente sulla sua persona, equivale a un divieto generale e non richiede che l'interessato cerchi proattivamente di opporsi a tale decisione[606].

Nondimeno, ai sensi del RGPD, il processo decisionale automatizzato che pro- duce effetti giuridici o che incide significativamente sulle persone può essere accettabile se è necessario per la conclusione o l'esecuzione di un contratto tra il titolare del trattamento e l'interessato o se quest 'ultimo ha prestato un consenso esplicito. Inoltre, il processo decisionale automatizzato è accet- tabile se è autorizzato per legge e se i diritti, le libertà e i legittimi interessi dell'interessato sono adeguatamente garantiti[607].

Il RGPD prevede inoltre che, tra gli obblighi del titolare del trattamento per quanto riguarda le informazioni da fornire in caso di raccolta di dati per- sonali, gli interessati debbano essere informati dell'esistenza di un processo decisionale automatizzato, compresa la profilazione[608]. Il diritto di accesso ai dati personali trattati dal titolare del trattamento rimane impregiudicato[609]. Le informazioni non dovrebbero indicare solo che la profilazione avrà luogo, ma dovrebbero altresì contenere informazioni significative sulla logica utiliz- zata nella profilazione e sulle conseguenze previste per i soggetti del tratta- mento[610]. Ad esempio, una compagnia di assicurazione malattia che utilizza processi decisionali automatizzati per le domande, dovrebbe fornire agli inter- essati informazioni generali sulle modalità di funzionamento dell'algoritmo e quali fattori l'algoritmo utilizza per calcolare i premi assicurativi. Allo stesso modo, nell'esercizio del loro «diritto di accesso», gli interessati possono rich- iedere al titolare del trattamento informazioni in merito all'esistenza di processi decisionali automatizzati e informazioni significative sulla logica utilizzata[611].

Le informazioni fornite agli interessati hanno lo scopo di assicurare la tras- parenza e consentire agli interessati di fornire consapevolmente un consenso, se opportuno, o di ottenere l'intervento umano. Il titolare del trattamento dei dati è tenuto ad attuare

misure appropriate per tutelare i diritti, le libertà e gli interessi legittimi dell’interessato. Questo comprende almeno il diritto di otte- nere l’intervento umano da parte del titolare del trattamento e la possibilità per l’interessato di esprimere la propria opinione e di contestare una decisione basata sul trattamento automatizzato dei propri dati personali[612].

Il Gruppo di lavoro articolo 29 ha fornito ulteriori orientamenti sull’utilizzo dei processi decisionali automatizzati ai sensi del RGPD[613].

Nell’ambito del diritto del CdE, le persone hanno il diritto di non essere oggetto di decisioni che le coinvolgano in maniera significativa, basate esclusiva- mente sul trattamento automatizzato, senza tenere in considerazione la loro

opinione[614]. L’obbligo di prendere in considerazione il parere dell’interessato quando le decisioni sono basate esclusivamente su un trattamento automa- tizzato significa che l’interessato ha il diritto di impugnare tali decisioni e di contestare eventuali inesattezze nei dati personali utilizzati dal titolare del trattamento e di contestare la pertinenza del profilo applicato[615]. Tuttavia, una persona non può esercitare tale diritto se la decisione automatizzata è autorizzata da una legge cui è soggetto il titolare del trattamento e che sta- bilisce anche misure adeguate per salvaguardare i diritti, le libertà e gli inter- essi legittimi dell’interessato. Inoltre, gli interessati hanno il diritto di ottenere, su richiesta, conoscenza del ragionamento alla base del trattamento dei dati effettuato[616]. La relazione esplicativa della Convenzione n. 108 modernizzata fornisce l’esempio di valutazione dell’affidabilità creditizia. Le persone dovreb- bero avere il diritto non solo di essere informate in merito alla decisione in sé, risultante dalla valutazione, ma anche di conoscere la *logica* alla base del trattamento dei loro dati personali, che ha portato a tale decisione. «La com- prensione di questi elementi contribuisce all’esercizio effettivo di altre garan- zie fondamentali, come il diritto di opposizione e il diritto di ricorso dinanzi ad un’autorità competente»[617].

La raccomandazione sulla profilazione, sebbene non giuridicamente vincolante, specifica le condizioni per la raccolta e il trattamento dei dati personali nel contesto della profilazione[618]. Essa contiene disposizioni sulla necessità di garantire che il trattamento nel contesto della profilazione sia equo, legittimo, propor- zionato ed abbia finalità determinate e legittime. Contiene inoltre disposizioni sulle informazioni che i titolari del trattamento dovrebbero fornire agli interes- sati. È contemplato nella raccomandazione anche il principio della qualità dei dati, che impone ai titolari del trattamento di adottare misure finalizzate a cor- reggere i fattori che comportano inesattezze, minimizzare i rischi o gli errori che la profilazione può comportare, e valutare periodicamente la qualità dei dati e gli algoritmi utilizzati.

6.2. Mezzi di ricorso, responsabilità, sanzioni e risarcimento

- In base alla Convenzione n. 108 modernizzata, il diritto nazionale delle parti con- traenti deve prevedere opportuni ricorsi e sanzioni contro le violazioni del diritto alla protezione dei dati.

- Nell'UE, il RGPD prevede mezzi di ricorso per gli interessati in caso di violazione dei loro diritti nonché sanzioni a carico dei titolari del trattamento e dei respon- sabili del trattamento che non rispettano le disposizioni del regolamento. Esso prevede anche il diritto al risarcimento e la responsabilità.

- L'interessato ha il diritto di proporre reclamo all'autorità di controllo con rifer- imento a presunte violazioni del regolamento così come il diritto a un ricorso giurisdizionale effettivo e il diritto di ottenere un risarcimento.

- Nell'esercizio del loro diritto a un ricorso effettivo, le persone possono essere rappresentate da organizzazioni senza scopo di lucro attive nel settore della protezione dei dati.

- Al titolare del trat tamento o al responsabile del trat tamento incombe la responsabilità per

qualsiasi danno materiale o immateriale causato dalla violazione.

- Le autorità di controllo hanno il potere di infliggere sanzioni amministrative pecuniarie per violazioni del regolamento fino a 20 000 000 di EUR o, per le imprese, il 4 % del fatturato mondiale totale annuo, se superiore.

- In caso di violazioni della normativa sulla tutela dei dati, in ultima istanza e nel rispetto di talune condizioni, gli interessati possono adire la Corte EDU.

- Ogni persona fisica o giudirica ha il diritto di presentare ricorso nei confronti di qualsiasi decisione del Comitato europeo per la protezione dei dati dinanzi alla CGUE, alle condizioni previste nei trattati.

L'adozione di strumenti giuridici non è sufficiente per garantire la protezione dei dati personali in Europa. Per rendere effettive le norme europee in materia di protezione dei dati, occorre istituire meccanismi che permettano alle per- sone di opporsi alle violazioni dei loro diritti e chiedere il risarcimento per i danni subiti. È altresì importante che le autorità di controllo dispongano del potere di irrogare sanzioni che siano efficaci, dissuasive e proporzionate ris- petto alla violazione in questione.

I diritti in materia di protezione dei dati possono essere esercitati dalla persona i cui diritti sono in gioco; tale persona è l'interessato. Tuttavia, anche altre per- sone, che soddisfino i requisiti necessari ai sensi del diritto nazionale, possono rappresentare gli interessati nell'esercizio dei loro diritti. Nell'ambito di diverse legislazioni nazionali, i minori e le persone con disabilità mentali devono essere rappresentate dai loro tutori[619]. Nell'ambito della normativa dell'UE in materia di protezione dei dati, un'associazione, la cui finalità legittima sia la promozione dei diritti in materia di protezione dei dati, può assumere la rappresentanza degli interessati dinanzi a un'autorità di controllo o dinanzi a un tribunale[620].

6.2.1. Diritto di proporre reclamo a un'autorità di controllo

Nell'ambito del diritto sia del CdE sia dell'UE, le persone hanno il diritto di presen- tare richieste e proporre reclami all'autorità di controllo, qualora ritengano che il trattamento dei loro dati personali non sia effettuato in conformità della legge.

La Convenzione n. 108 modernizzata riconosce il diritto degli interessati di ricorrere all'assistenza di un'autorità di controllo nell'esercizio dei loro diritti ai sensi della Convenzione, a prescindere dalla loro nazionalità o dalla loro res- idenza[621]. Le richieste di assistenza possono essere respinte solo in circostanze eccezionali e gli interessati non

dovrebbero coprire i costi e le spese connessi all'assistenza[622].

Disposizioni analoghe si trovano nell'ordinamento giuridico dell'UE. Il RGPD impone alle autorità di controllo di adottare misure per agevolare la propo- sizione di reclami, ad esempio predisponendo un modulo per la proposizione dei reclami con mez zi elet tronici[623]. L'interessato può proporre il reclamo all'autorità di controllo nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione[624]. I reclami devono

essere oggetto di indagine e l'autorità di controllo deve informare l'interessato dell'esito del procedimento relativo al reclamo[625].

Potenziali violazioni da parte di istituzioni o organismi dell'UE possono essere sottoposte all'attenzione del Garante europeo della protezione dei dati[626]. La mancata risposta del GEPD entro sei mesi equivale a una decisione di rigetto del reclamo. I ricorsi contro le decisioni del GEPD possono essere proposti dinanzi alla CGUE, nel quadro del regolamento (CE) n. 45/2001, che impone alle istituzioni e agli organismi dell'UE l'osservanza delle norme in materia di protezione dei dati.

Le decisioni delle autorità nazionali di controllo devono poter essere oggetto di ricorso giurisdizionale. Ciò vale sia per l'interessato sia per i titolari del tratta- mento e i responsabili del trattamento che sono stati parti di un procedimento dinanzi all'autorità di controllo.

Esempio: nel settembre 2017, l'autorità spagnola per la protezione dei dati ha multato Facebook per aver violato diverse norme di protezione dei dati. L'autorità di controllo ha condannato il social network per avere raccolto, archiviato e trattato dati personali, comprese categorie particolari di dati personali a fini pubblicitari e senza ottenere il

consenso dell'interessato. La decisione si basava su un'indagine condotta dall'autorità di controllo di propria iniziativa.

6.2.2. Diritto a un ricorso giurisdizionale effettivo

Oltre al diritto di proporre reclamo dinanzi all'autorità di controllo, le per- sone devono avere il diritto a un ricorso giurisdizionale effettivo e il diritto di proporre ricorso dinanzi a un tribunale. Il diritto a un ricorso giurisdizionale è fortemente radicato nella tradizione giuridica europea ed è riconosciuto come

diritto fondamentale ai sensi sia dell'articolo 47 della Carta dei diritti fonda- mentali dell'UE sia dell'articolo 13 della CEDU[627].

Nell'ambito del diritto dell'UE, l'importanza di garantire agli interessati ricorsi giurisdizionali effettivi in caso di violazione dei loro diritti risulta chiaramente sia nelle disposizioni del RGPD (che sancisce il diritto a un ricorso giurisdizion- ale effettivo avverso le autorità di controllo e i titolari e i responsabili del trat- tamento) sia nella giurisprudenza della CGUE.

Esempio: nella causa *Schrems*[628], la CGUE ha dichiarato l'invalidità della decisione di adeguatezza «approdo sicuro». Tale decisione aveva consentito trasferimenti internazionali di dati dall'UE a organizzazioni negli Stati Uniti, che si erano autocertificate nell'ambito del regime dell'approdo sicuro. La CGUE ha ritenuto che il regime dell'approdo sicuro presentasse numerosi punti deboli, che pregiudicavano i diritti fondamentali dei cittadini dell'UE alla protezione della vita privata e dei dati personali e il diritto a un ricorso giurisdizionale effettivo.

Per quanto riguarda la violazione dei diritti alla vita privata e alla protezione dei dati, la CGUE ha sottolineato che la legislazione statunitense consentiva a talune autorità pubbliche di accedere ai

dati personali trasferiti dagli Stati membri verso gli Stati Uniti, e di trattarli in maniera incompatibile con le finalità originarie del loro trasferimento e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale. Per quanto riguarda il diritto a un ricorso effettivo, essa ha constatato che non esistevano, per gli interessati, rimedi amministrativi o giurisdizionali che consentissero di accedere ai dati che li riguardavano e, eventualmente, di ottenerne la rettifica o la soppressione. La CGUE ha concluso che una normativa che non prevede alcuna possibilità di avvalersi di rimedi giuridici al fine di accedere a dati personali o ottenerne la rettifica o la soppressione, «non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta». Essa ha sottolineato che l'esistenza di un ricorso giurisdizionale che assicuri il rispetto delle disposizioni di legge, è inerente all'esistenza di uno Stato di diritto.

Le persone, i titolari del trattamento o i responsabili del trattamento che inten- dono impugnare una decisione giuridicamente vincolante di un'autorità di con- trollo possono proporre ricorso dinanzi a un tribunale[629]. Il termine «decisione» dovrebbe essere interpretato in senso lato e comprendere l'esercizio, da parte delle autorità di controllo, di poteri di indagine, correttivi e sanzionatori nonché le decisioni di archiviare o respingere un reclamo. Tuttavia, le misure che non sono giuridicamente vincolanti, come pareri o consulenza forniti dall'autorità di controllo, non possono essere oggetto di ricorso dinanzi a un tribunale[630]. Le azioni legali sono promosse dinanzi ai tribunali dello Stato membro in cui la pertinente autorità di controllo è stabilita[631].

Nei casi in cui un titolare del trattamento o un responsabile del trattamento abbiano violato i diritti di un interessato, quest'ultimo ha il diritto di proporre ricorso dinanzi a un tribunale[632]. Nelle azioni contro un titolare del trat ta- mento o responsabile del trat tamento, è par ticolarmente impor tante che i sing oli abbia no la possibilit à di scegliere dove av via re l'azione legale. Essi possono scegliere di agire nello Stato membro in cui il titolare del trat- tamento o il responsabile del trattamento ha uno stabilimento o nello Stato membro in cui l'interessato risiede abitualmente[633]. La seconda possibilità facilita

notevolmente le persone nell’esercizio dei loro diritti, in quanto con- sente loro di promuovere azioni nello Stato in cui risiedono e all’interno di una giurisdizione loro familiare. Limitare i procedimenti avverso i titolari del trat- tamento e i responsabili del trattamento allo Stato membro in cui essi hanno una sede, potrebbe scoraggiare gli interessati risiedenti in altri Stati membri dall’intentare un’azione giudiziaria, dal momento che comporterebbe spese di viaggio e costi supplementari, e il procedimento potrebbe svolgersi in una lin- gua e in una giurisdizione straniere. L’unica eccezione riguarda i casi in cui il titolare del trattamento o il responsabile del trattamento sono autorità pub- bliche e il trattamento è effettuato nell’esercizio dei pubblici poteri. In questo caso, sono competenti per il ricorso solo i tribunali dello Stato dell’autorità pub- blica pertinente[634].

Anche se nella maggior parte dei casi le cause riguardanti le norme sulla pro- tezione dei dati saranno decise presso i tribunali degli Stati membri, alcune

cause potrebbero essere promosse dinanzi alla CGUE. La prima ipotesi è quando un interessato, un titolare del trattamento o un responsabile del trattamento oppure un'autorità di controllo, presenta ricorso per l'annullamento di una decisione del CEPD. L'azione, tuttavia, è assoggettata alle condizioni dell'articolo 263 del TFUE, il che significa che, affinché sia ammissibile, tali persone ed entità devono dimostrare che la decisione del comitato si riferisce direttamente e individualmente alle stesse.

Il secondo scenario riguarda i casi di trattamento illecito di dati personali da parte di istituzioni o organismi dell'UE. Se le istituzioni dell'UE violano la legge sulla protezione dei dati, gli interessati possono presentare ricorso diret- tamente dinanzi al Tribunale dell'UE (il Tribunale fa parte della CGUE). Il Tri- bunale è responsabile, in prima istanza, dei reclami riguardanti violazioni del diritto dell'UE da parte di istituzioni dell'UE. Pertanto, i ricorsi proposti avverso il GEPD - in quanto istituzione dell'UE - possono essere proposti anche dinanzi al Tribunale[635].

Esempio: nella causa *Bavarian Lager*[636], la società aveva chiesto alla Commissione europea l'accesso ai verbali completi di una riunione tenuta dalla Commissione, asseritamente concernente questioni giuridiche rilevanti per tale società. La Commissione aveva respinto la richiesta di accesso

della società per prevalenti interessi di protezione dei dati[637]. La Bavarian Lager aveva proposto, ai sensi dell'articolo 32 del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, un ricorso contro tale decisione dinanzi al Tribunale di primo grado (il predecessore del Tribunale). Nella sua decisione (causa T-194/04, *The Bavarian Lager Co. Ltd c. Commissione delle Comunità europee)*, il Tribunale di primo grado aveva annullato la decisione con la quale la Commissione respingeva la richiesta di accesso. La Commissione europea aveva rinviato la causa dinanzi alla CGUE.

La CGUE (riunita in Grande Sezione) ha emanato una sentenza di annullamento della sentenza del Tribunale di primo grado e di conferma del rigetto da parte della Commissione europea della richiesta di accesso ai verbali integrali della

riunione, allo scopo di proteggere i dati personali delle persone presenti alla riunione. La CGUE ha ritenuto che la Commissione abbia agito correttamente rifiutando di divulgare tali informazioni, dal momento che i partecipanti non avevano prestato il loro consenso alla divulgazione dei loro dati personali. Inoltre, la Bavarian Lager non aveva dimostrato la necessità di accedere a tali informazioni.

Infine, gli interessati, le autorità di controllo, i titolari del trattamento o i respon- sabili del trattamento possono, nel corso di procedimenti nazionali, rivolgersi al giudice nazionale affinché chieda chiarimenti alla CGUE sull'interpretazione e sulla validità di atti delle istituzioni, degli organismi, degli uffici o delle agen- zie dell'UE. Tali chiarimenti sono noti come pronunce pregiudiziali. Non si tratta di un ricorso diretto a disposizione del denunciante, ma di un ricorso che con- sente ai giudici nazionali di assicurare che la loro interpretazione del diritto dell'UE sia corretta. È grazie a questo meccanismo di pronunce pregiudiziali che la CGUE è stata investita di cause fondamentali, quali *Digital Rights Ireland* e *Kärntner Landesregierung e a.*[638] e *Schrems*[639], che hanno inciso grandemente sull'evoluzione del diritto dell'UE in materia di protezione dei dati.

Esempio: *Digital Rights Ireland e Kärntner Landesregierung e a.*[640] avevano presentato una

causa riunita alla High Court irlandese e alla corte costituzionale austriaca, riguardante la conformità della direttiva 2006/24/CE (direttiva sulla conservazione dei dati) con la normativa dell'UE in materia di protezione dei dati. La corte costituzionale austriaca aveva sottoposto alla CGUE alcune questioni vertenti sulla validità degli articoli da 3 a 9 della direttiva 2006/24/CE alla luce degli articoli 7, 9 e 11 della Carta dei diritti fondamentali dell'UE. Tra queste, vie era la questione se talune disposizioni della legge federale austriaca sulle telecomunicazioni che trasponevano la direttiva sulla conservazione dei dati, fossero incompatibili con alcuni aspetti dell'ex direttiva sulla tutela dei dati e del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE.

Nella causa *Kärntner Landesregierung e a.*, il sig. Seitlinger, uno dei ricorrenti nel procedimento pendente dinanzi alla corte costituzionale, aveva dichiarato di usare il telefono, Internet e la posta elettronica, sia sul lavoro sia nella vita privata. Di conseguenza, le informazioni che egli aveva inviato e ricevuto erano passate attraverso reti di telecomunicazione pubbliche. Ai sensi della legge austriaca sulle telecomunicazioni del 2003, il suo fornitore di servizi di telecomunicazione era obbligato, per legge, a raccogliere e a conservare i dati relativi all'uso della rete. Il sig. Seitlinger riteneva che la raccolta e la conservazione dei suoi dati personali non fossero necessarie ai fini tecnici di inviare e ricevere informazioni attraverso la rete. Né erano necessarie, in effetti, la raccolta e la conservazione di tali dati a fini di fatturazione. Il sig. Seitlinger aveva dichiarato di non avere acconsentito a tale uso dei suoi dati personali, il solo motivo della cui raccolta e conservazione era la legge austriaca sulle telecomunicazioni del 2003.

Il sig. Seitlinger aveva pertanto adito la corte costituzionale austriaca, sostenendo che gli obblighi di legge imposti al fornitore dei servizi di telecomunicazione avevano violato i suoi diritti fondamentali ai sensi dell'articolo 8 della Carta dei diritti fondamentali dell'UE. Dal momento che la legislazione austriaca attuava il diritto dell'UE (l'allora direttiva sulla

conservazione dei dati), la corte costituzionale austriaca aveva sottoposto la questione alla CGUE, affinché si pronunciasse in merito alla compatibilità della direttiva con i diritti alla vita privata e alla protezione dei dati, sanciti dalla Carta dei diritti fondamentali dell'UE.

La Grande Sezione della CGUE si è pronunciata sulla causa e la sua decisione ha condotto all'annullamento della direttiva dell'UE sulla conservazione dei dati. La CGUE ha ritenuto che la direttiva comportasse un'ingerenza di particolare gravità nei diritti fondamentali alla vita privata e alla protezione dei dati, senza che siffatta ingerenza fosse limitata a quanto strettamente necessario. La direttiva perseguiva un obiettivo legittimo, in quanto conferiva alle autorità nazionali possibilità supplementari di indagare e perseguire reati gravi e costituiva, pertanto, uno strumento utile per le indagini penali. Nondimeno, la CGUE ha osservato che le limitazioni ai diritti fondamentali dovrebbero applicarsi solo se strettamente necessarie e dovrebbero essere affiancate da norme chiare e precise che ne disciplinino la portata, nonché da garanzie a tutela delle persone.

Secondo la CGUE, la direttiva non soddisfaceva tale criterio di necessità. In primo luogo, essa non prevedeva norme chiare e precise che limitassero la portata dell'ingerenza. Anziché imporre una relazione tra dati conservati e reati gravi, la direttiva si applicava a tutti i metadati di tutti gli utenti di tutti i mezzi di comunicazione elettronica. Essa costituiva, pertanto, un'ingerenza nei diritti alla vita privata e alla protezione dei dati della quasi totalità della popolazione dell'UE, che poteva essere considerata non proporzionata. Essa non conteneva condizioni volte a limitare l'accesso ai dati personali da parte delle persone autorizzate né tale accesso era soggetto a condizioni procedurali, quali il requisito dell'approvazione da parte di un'autorità amministrativa o tribunale prima dell'accesso. Infine, la direttiva non prevedeva garanzie chiare per la protezione dei dati conservati. Essa non assicurava, pertanto, una protezione efficace dei dati contro i il rischio di abuso nonché contro eventuali accessi e usi illeciti dei dati[641].

In linea di principio, la CGUE deve rispondere alle questioni che le vengono sot- toposte e non può rifiutare di pronunciarsi in via pregiudiziale sulla base del fatto che la sua risposta non sarebbe pertinente né tempestiva rispetto alla causa originaria. Tuttavia, essa può rifiutarsi qualora la domanda esuli dalla propria sfera di competenza[642]. La CGUE delibera solo sugli

elementi costitutivi della questione pregiudiziale, mentre il giudice nazionale conserva la propria competenza a decidere la causa originale[643].

Ai sensi del diritto del CdE, ciascuna parte si impegna a stabilire sanzioni e ricorsi giudiziali ed extragiudiziali adeguati in caso di violazioni delle dispo- sizioni della Convenzione n. 108 modernizzata[644]. Inoltre, asserzioni nei con- fronti di una parte contraente della CEDU per violazione dei diritti di protezione dei dati ai sensi dell'articolo 8 della stessa, possono essere fatte valere dinanzi alla Corte EDU quando tutte le vie di ricorso nazionali sono esaurite. Un ricorso dinanzi alla Corte EDU per violazione dell'articolo 8 della CEDU deve soddisfare anche altri criteri di ammissibilità (articoli 34 e 35 della CEDU)[645].

Benché possano essere dirette solo contro le parti contraenti, le domande pre- sentate alla Corte EDU possono riguardare indirettamente anche azioni o omis- sioni di privati, nella misura in cui una parte contraente non abbia adempiuto ai propri obblighi a norma della CEDU e non abbia garantito una protezione suf- ficiente contro le violazioni dei diritti alla protezione dei dati nel proprio ordina- mento nazionale.

Esempio: nella causa *K. U. c. Finlandia*[646], il ricorrente, un minore, aveva denunciato la pubblicazione a suo nome di un annuncio a sfondo sessuale su un sito Internet di incontri. Il fornitore di servizi non aveva rivelato l'identità della persona che aveva pubblicato i dati a causa degli obblighi di riservatezza imposti dalla legge finlandese. Il ricorrente lamentava l'assenza nella legislazione finlandese di strumenti adeguati a consentirgli di tutelarsi contro le azioni commesse da un privato che aveva pubblicato in Internet dati compromettenti che lo riguardavano. La Corte EDU ha stabilito che gli Stati non solo erano obbligati ad astenersi da ingerenze arbitrarie nella vita privata degli individui, ma erano anche soggetti a obblighi positivi, che comportano
«l'adozione di misure atte a garantire il rispetto della vita privata anche nella sfera dei rapporti reciproci fra gli individui». Nel caso di specie, affinché il ricorrente fosse protetto all'atto pratico e in modo

efficace, s’imponeva che fossero presi provvedimenti reali per identificare e perseguire l’autore del reato. Tuttavia, lo Stato non aveva garantito tale protezione e la Corte ha concluso asserendo una violazione dell’articolo 8 della CEDU.

Esempio: nella causa *Köpke c. Germania*[647], la ricorrente era stata sospettata di furto sul luogo di lavoro e sottoposta di nascosto a videosorveglianza. La Corte EDU ha concluso che «nulla indicava che le autorità nazionali non avessero cercato un equo equilibrio, nell’ambito del loro margine di discrezionalità, fra il diritto della ricorrente al rispetto della propria vita privata di cui all’articolo 8 da una parte e, dall’altra, l’interesse del datore di lavoro alla protezione dei propri diritti di proprietà nonché l’interesse pubblico alla corretta amministrazione della giustizia». Pertanto, la domanda è stata dichiarata irricevibile.

Se la Corte EDU constata che una parte contraente ha violato uno qualsiasi dei diritti sanciti dalla CEDU, detta parte è tenuta ad attuare la sentenza della Corte EDU (articolo 46 della CEDU). Le misure di esecuzione devono dapprima fare ces- sare la violazione e porre rimedio, per quanto possibile, alle conseguenze nega- tive a carico del ricorrente. L'esecuzione delle sentenze può anche richiedere misure generali per prevenire violazioni simili a quelle constatate dalla Corte, attraverso modifiche legislative, pronunce giurisprudenziali o altre misure.

Se la Corte EDU constata che vi è stata una violazione della CEDU, l'articolo 41 della CEDU prevede che la Corte possa accordare un'«equa soddisfazione» alla parte lesa a spese della parte contraente.

Diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro

Il RGPD consente alle persone che propongono reclamo a un'autorità di con- trollo o intentano un'azione dinanzi a un tribunale, di dare mandato a un organ- ismo, un'organizzazione o un'associazione senza scopo di lucro[648]. Tali entità senza scopo di lucro devono avere obiettivi statutari di pubblico interesse ed essere attive nel settore della protezione dei dati. Esse possono proporre rec- lamo o esercitare il diritto a un ricorso

giurisdizionale per conto dell'interessato o degli interessati. Il regolamento lascia agli Stati membri la scelta di decidere, conformemente al diritto nazionale, se un organismo possa proporre reclami per conto di interessati, senza avere ricevuto mandato dagli stessi.

Tale diritto di rappresentanza consente agli individui di beneficiare dell'esperienza e delle capacità organizzative e finanziarie di tali entità senza scopo di lucro, facilitando considerevolmente le persone nell'esercizio dei loro diritti. Il RGPD consente a tali entità di intentare azioni collettive per conto di diversi interes- sati. Ciò giova anche al funzionamento e all'efficienza del sistema giudiziario, dal momento che azioni simili sono raggruppate ed esaminate insieme.

6.2.3. Responsabilità e diritto al risarcimento

Il diritto a un ricorso effettivo deve consentire alle persone di chiedere un risar- cimento per i danni subiti a causa del trattamento dei propri dati personali,

effettuato con modalità non conformi alla legislazione applicabile. La respon- sabilità dei titolari del trattamento e dei responsabili del trattamento in caso di trattamento illecito è riconosciuta esplicitamente nel RGPD[649]. Il regolamento riconosce alle persone il diritto di ottenere dal titolare del trattamento o dal responsabile del trattamento il risarcimento per i danni materiali o immateriali subiti, mentre i considerando stabiliscono che «il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento»[650]. I titolari del trattamento sono responsabili e possono essere oggetto di richieste di risarcimento, se non adempiono i loro obblighi ai sensi del regolamento. I responsabili del trattamento dei dati personali rispondono per il danno cagionato dal trattamento solo se non hanno ottemperato agli obblighi del regolamento specificatamente diretti ai responsabili del trat- tamento o hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato l'intero risarcimento del danno, il RGPD stabilisce che tale titolare del trattamento o responsabile del tratta- mento possa reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento cor- rispondente al loro

grado di responsabilità per il danno[651]. Al contempo, le deroghe alla responsabilità sono molto rigorose e subordinate alla dimostrazi- one che l’evento dannoso non è in alcun modo imputabile al titolare del trat- tamento o al responsabile del trattamento.

Il risarcimento deve essere «pieno ed effettivo» rispetto al danno subito. Qualora più titolari o responsabili dello stesso trattamento siano responsabili del danno causato, ogni titolare del trattamento o responsabile del trattamento deve rispondere per la totalità del danno. Questa norma mira a garantire un risarcimento effettivo degli interessati e un approccio coordinato, rispetto alla conformità, da parte dei titolari e dei responsabili del trattamento coinvolti nelle attività di trattamento.

Esempio: gli interessati non sono tenuti a presentare ricorso e richiedere un risarcimento a tutte le entità responsabili del danno, in quanto ciò potrebbe comportare procedimenti lunghi e costosi. È sufficiente presentare ricorso

avverso uno dei contitolari del trattamento, il quale può quindi essere tenuto a rispondere per la totalità del danno. In tali casi, un titolare del trattamento o un responsabile del trattamento che risarcisce il danno ha successivamente il diritto di recuperare l'importo pagato dalle altre entità coinvolte nel trattamento e responsabili della violazione, per la loro parte di responsabilità per il danno. Tali procedimenti tra i diversi contitolari del trattamento e responsabili del trattamento hanno luogo dopo l'ottenimento del risarcimento da parte dell'interessato e quest'ultimo non ne è parte.

Nel quadro giuridico del CdE, l'articolo 12 della Convenzione n. 108 moderniz- zata impone alle parti contraenti di stabilire mezzi di ricorso appropriati con riferimento alle violazioni della legislazione nazionale d'attuazione delle pre- scrizioni della Convenzione. La relazione esplicativa della Convenzione n. 108 modernizzata specifica che i ricorsi devono prevedere la possibilità di contes- tare in via giudiziaria una decisione o una prassi, pur dovendo essere messi a disposizione anche mezzi di ricorso extragiudiziali[652]. Le modalità e le diverse norme associate all'accesso a tali mezzi di ricorso, unitamente alla procedura da seguire, sono lasciate alla discrezione di ciascuna parte contraente. Le parti contraenti e i giudici nazionali dovrebbero altresì prevedere disposizioni riguar- danti la compensazione finanziaria per i danni materiali e

immateriali causati dal trattamento nonché la possibilità di ricorsi collettivi[653].

6.2.4. Sanzioni

Nell'ambito del diritto del CdE, l'articolo 12 della Convenzione n. 108 mod- ernizzata prevede che ciascuna parte contraente debba definire le sanzioni e i ricorsi appropriati per le violazioni delle disposizioni di diritto nazionale che danno attuazione ai principi fondamentali della protezione dei dati enunciati nella Convenzione n. 108. La Convenzione non stabilisce né impone una parti- colare serie di sanzioni. Al contrario, specifica chiaramente che ciascuna parte contraente ha la facoltà di determinare la natura delle sanzioni giurisdizionali o non giurisdizionali, che possono essere penali, amministrative o civili. La relazi- one esplicativa della Convenzione n. 108 modernizzata prevede che le san- zioni debbano essere efficaci, proporzionate e dissuasive[654]. Le parti contraenti

devono rispettare tale principio nel determinare la natura e la gravità delle sanzioni disponibili nel loro ordinamento giuridico interno.

Nell'ambito del diritto dell'UE, l'articolo 83 del RGPD autorizza le autorità di controllo degli Stati membri a infliggere sanzioni amministrative pecuniarie in relazione a violazioni del regolamento. Il livello delle sanzioni e le circos- tanze delle quali le autorità nazionali tengono conto nel decidere se infliggere una sanzione, nonché il tetto massimo di tali sanzioni sono anch'essi fissati nell'articolo 83. Il regime sanzionatorio è pertanto armonizzato in tutta l'UE.

Nell'infliggere le sanzioni, il RGPD segue un approccio a più livelli. Le autorità di controllo hanno il potere di infliggere sanzioni amministrative pecuniarie per violazioni del regolamento fino a 20 000 000 di EUR o, per le imprese, il 4 % del fatturato mondiale totale annuo, se superiore. Le violazioni che possono comportare questo livello di sanzioni includono le violazioni dei principi fon- damentali del trattamento e le condizioni relative al consenso, le violazioni dei diritti degli interessati e delle disposizioni del regolamento che disciplinano il trasferimento di dati personali a destinatari in paesi terzi. Per altre violazioni, le autorità di controllo possono infliggere sanzioni fino a 10 000 000 di EUR o, per le imprese, fino al 2 % del fatturato mondiale totale annuo, se superiore.

Nel decidere il tipo e il livello della sanzione da infliggere, le autorità di con- trollo devono tenere conto di diversi elementi[655]. Ad esempio, devono tenere debito conto della natura, gravità e durata della violazione, delle categorie di dati personali interessate e del carattere doloso o colposo della violazione. Se un titolare del trattamento ha adottato misure per attenuare il danno subito dagli interessati, deve esserne tenuto conto. Analogamente, il grado di coop- erazione con l'autorità di controllo a seguito della violazione e la maniera in cui quest'ultima ha preso conoscenza della stessa (ad esempio, se è stata segnal- ata dall'entità responsabile del trattamento o da un interessato i cui diritti sono stati violati) sono altri fattori importanti che guidano le autorità di controllo nella loro decisione[656].

Oltre alla possibilità di imporre sanzioni am ministrative pecuniarie, le autorità di controllo hanno a disposizione una vasta gamma di altri poteri

correttivi. I cosiddetti poteri «correttivi» delle autorità di controllo sono sanciti dall'articolo 58 del RGPD. Essi vanno dall'emissione di ingiunzioni, avverti- menti e ammonimenti ai titolari del trattamento e ai responsabili del tratta- mento, all'imposizione di divieti temporanei o anche permaenti alle attività di trattamento.

Per quanto riguarda le sanzioni contro le violazioni del diritto dell'UE da parte delle istituzioni o degli organismi dell'UE, a causa della speciale competenza del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, le sanzioni possono essere previste sotto forma di provvedimenti disciplinari. A norma dell'articolo 49 del regolamento, «il funzionario o altro agente delle Comunità europee che, volontariamente o per negligenza, non assolva agli obblighi previsti dal presente regolamento è passibile di provvedimenti disci- plinari [...]».

Nell’ambito del diritto dell’UE, il regolamento generale sulla protezione dei dati prevede la libera circolazione di dati all’interno dell’UE. Tuttavia, esso contiene requisiti specifici relativi al trasferimento dei dati personali verso paesi terzi al di fuori dell’UE e organizzazioni internazionali. Il regolamento riconosce l’im- portanza di tali trasferimenti, specialmente in considerazione del commercio e della cooperazione internazionali, ma riconosce anche il maggiore rischio per i dati personali. Il regolamento mira pertanto a garantire, per i dati personali trasferiti verso paesi terzi, lo stesso livello di protezione garantito all’interno dell’UE[657]. Il diritto del CdE riconosce inoltre l’importanza delle norme di attua- zione per i flussi transfrontalieri di dati, basate sulla libera circolazione tra le parti e requisiti specifici per i trasferimenti verso parti non contraenti.

7.1. Natura dei trasferimenti di dati personali

- Il diritto dell’UE e il diritto del CdE prevedono entrambi norme sul trasferimento dei dati personali verso destinatari in paesi terzi o organizzazioni internazionali.

- Garantire la tutela dei diritti dell’interessato, quando i dati sono trasferiti al di fuori dell’UE, consente alla protezione prevista dal diritto dell’UE di seguire i dati personali provenienti dall’UE.

Nell’ambito del diritto del CdE, i flussi transfrontalieri di dati sono descritti come trasferimenti di dati personali verso destinatari soggetti a una giurisdi- zione straniera[658]. I flussi transfrontalieri di dati verso un destinatario che non sia soggetto alla giurisdizione di una parte contraente sono consentiti solo se è garantito un livello di protezione adeguato[659].

Il diritto dell’UE disciplina i trasferimenti «di dati personali oggetto di un trat- tamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un’organizzazione internazionale [...]»[660]. Tali flussi

di dati hanno luogo soltanto se sono conformi alle disposizioni di cui al capo V del RGPD.

I flussi transfrontalieri di dati personali sono consentiti verso un destinatario che sia soggetto alla giurisdizione di una parte contraente o di uno Stato mem- bro ai sensi del diritto dell'UE o del diritto del CdE, rispettivamente. Entrambi gli ordinamenti giuridici consentono inoltre il trasferimento dei dati verso un paese che non è parte contraente o Stato membro, a condizione che siano sod- disfatte determinate condizioni.

7.2. Libera circolazione/libero flusso di dati personali tra gli Stati membri o tra le parti contraenti

- Il flusso di dati personali in tutta l'UE nonché i trasferimenti di dati personali tra le parti contraenti della Convenzione n. 108 modernizzata devono essere esenti da restrizioni. Tuttavia, dal momento che non tutte le parti contraenti della Con- venzione n. 108 modernizzata sono Stati membri dell'UE, i trasferimenti da uno Stato membro dell'UE verso un paese terzo che è comunque parte contraente della Convenzione n. 108, sono possibili solo se soddisfano le condizioni stabilite nel RGPD.

Nell'ambito del diritto del CdE, la libera circolazione di dati personali tra le parti contraenti della Convenzione n. 108 modernizzata deve essere garantita. Tutta- via, il trasferimento può essere vietato se vi è il reale e serio rischio che il trasfe- rimento a terzi porti ad aggirare le disposizioni della Convenzione, e se una parte
«può agire in quanto vincolata da norme armonizzate in materia di tutela con- divise dagli Stati appartenenti a un'organizzazione internazionale regionale»[661].

Nell'ambito del diritto dell'UE, le restrizioni o i divieti alla libera circolazione dei dati personali fra Stati membri per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali sono vietati[662]. Lo spazio di libera circolazione dei dati è stato esteso dall'accordo sullo Spazio economico europeo (SEE)[663], che introduce l'Islanda, il Liechtenstein e la Norve- gia nel mercato interno.

Esempio: se un'affiliata di un gruppo d'imprese internazionale, con sede in diversi Stati membri, fra cui la Slovenia e la Francia, invia dati personali dalla Slovenia alla Francia, tale flusso di dati non dev'essere limitato o vietato dal diritto nazionale sloveno per motivi attinenti alla protezione dei dati personali.

Se, tuttavia, la medesima affiliata slovena intende trasferire gli stessi dati personali alla società madre in Malesia, l'esportatore di dati sloveno deve tenere conto delle disposizioni di cui al capo V del RGPD. Queste disposizioni mirano a salvaguardare i dati personali degli interessati che sono soggetti alla giurisdizione dell'UE.

Nell'ambito del diritto dell'UE, i flussi di dati personali verso gli Stati membri del SEE a fini di prevenzione, indagine, accertamento o perseguimento di reati o di esecuzione di sanzioni penali sono soggetti alla direttiva 2016/680[664]. Ciò garantisce anche che lo scambio di dati personali da parte delle autorità com- petenti all'interno dell'Unione non sia limitato o proibito per motivi di prote- zione dei dati. Ai sensi del diritto del CdE, il trattamento di tutti i dati perso- nali (compresi i flussi transfrontalieri con altre parti della Convenzione n. 108), senza eccezioni basate su finalità o campi d'azione, rientra nell'ambito della Convenzione n. 108, anche se le parti contraenti possono prevedere deroghe. Tutti i membri del SEE sono anche parti della Convenzione n. 108.

7.3. Trasferimenti di dati personali verso paesi terzi/parti non contraenti o organizzazioni internazionali

• Sia il CdE sia l'UE consentono il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché siano soddisfatte determinate condizioni a salvaguardia dei dati personali.

• Ai sensi del diritto del CdE, un livello di protezione adeguato può essere garantito dal diritto dello Stato o dell'organizzazione internazionale, oppure predisponendo standard adeguati.

• Nell'ambito del diritto dell'UE, i trasferimenti possono avere luogo se il paese terzo garantisce un livello adeguato di protezione o se il titolare del

trattamento o il responsabile del trattamento fornisce garanzie adeguate, fra cui diritti azionabili degli interessati e mezzi di ricorso giurisdizionali, che pos- sono consistere in clausole tipo per la protezione dei dati o norme vincolanti d'impresa.

• Il diritto del CdE e dell'UE prevede clausole di deroga che consentono il trasferi- mento di dati personali in specifiche circostanze, anche qualora non siano stati predisposti un livello di protezione adeguato né garanzie appropriate.

La legislazione del CdE e quella dell'UE consentono il flusso di dati verso paesi terzi o organizzazioni internazionali, ma stabiliscono condizioni diverse. Cia- scuna serie di condizioni tiene conto della diversa struttura e degli scopi della rispettiva organizzazione.

Nell'ambito del diritto dell'UE vi sono, in linea di principio, due modi per con- sentire il trasferimento di dati personali verso paesi terzi o organizzazioni inter- nazionali. I trasferimenti di dati personali possono avvenire sulla base di una decisione di adeguatezza della Commissione europea[665] o, in mancanza di tale decisione di adeguatezza, se il titolare del trattamento o il responsabile del trattamento fornisce garanzie appropriate, compresi diritti azionabili e mezzi di ricorso giurisdizionali per

l'interessato[666]. In mancanza di una decisione di ade- guatezza o di garanzie adeguate, sono previste diverse deroghe.

Ai sensi del diritto del CdE, tuttavia, il libero trasferimento dei dati verso parti non contraenti della Convenzione è consentito solo sulla base:

- della legislazione di tale Stato o dell'organizzazione internazionale, com- presi i trattati o gli accordi internazionali applicabili che offrano garanzie adeguate;

- di tutele ad hoc o standardizzate approvate, fornite da strumenti giuridi- camente vincolanti, adottati e attuati dalle persone coinvolte nel trasferi- mento e nell'ulteriore trattamento[667].

Analogamente al diritto dell'UE, in mancanza di un livello di protezione dei dati adeguato, sono previste diverse deroghe.

7.3.1. Trasferimento sulla base di una decisione di adeguatezza

Nell’ambito del diritto dell’UE, la libera circolazione dei dati personali verso paesi terzi con un adeguato livello di protezione di detti dati è prevista dall’articolo 45 del RGPD. La CGUE ha precisato che il termine «livello di protezione adeguato» impone al paese terzo di garantire un livello di protezione dei diritti e delle libertà fondamentali «sostanzialmente equivalente»[668] alle garanzie previste dalla legislazione dell’UE. Allo stesso tempo, i mezzi dei quali il paese terzo si avvale al fine di garantire tale livello di protezione possono essere diversi da quelli attuati all’interno dell’UE; il livello di adeguatezza non com- porta necessariamente una duplicazione pedissequa delle norme dell’UE[669].

La Commissione europea valuta il livello di protezione dei dati in paesi stranieri esaminando la loro legislazione nazionale e gli obblighi internazionali appli- cabili. Occorre altresì tener conto della partecipazione di un paese ai sistemi multilaterali o regionali, in particolare per quanto riguarda la protezione dei dati personali. Se la Commissione europea ritiene che il paese terzo, o l’orga- nizzazione internazionale, garantisce un livello adeguato di protezione, può emettere una decisione di adeguatezza con effetto vincolante[670]. Nondimeno, la CGUE ha dichiarato che le autorità nazionali di controllo restano competenti per esaminare la domanda di una persona relativa alla

tutela dei dati personali della stessa, i quali sono stati trasferiti verso un paese terzo che la Commis- sione ha ritenuto garantire un livello di protezione adeguato, qualora tale per- sona faccia valere che il diritto e la prassi vigenti nel paese terzo non offrono un livello di protezione dei dati personali sufficiente[671].

La Commissione europea può altresì valutare l'adeguatezza di un territorio all'interno di un paese terzo o limitarsi a settori specifici, come, ad esempio,

nel caso del diritto commerciale privato del Canada[672]. Esistono inoltre consta- tazioni di adeguatezza per i trasferimenti basati su accordi tra l'UE e paesi terzi. Tali decisioni riguardano esclusivamente un solo tipo di trasferimento di dati, quali la trasmissione dei codici di prenotazione (PNR) da parte di una compa- gnia aerea alle autorità straniere preposte ai controlli di frontiera nei casi in cui la compagnia aerea operi partendo dall'UE, dirigendosi verso alcune destina- zioni extra-europee (cfr. la sezione 7.3.4).

Le decisioni di adeguatezza sono soggette a controlli su base continuativa. La Commissione europea esamina periodicamente tali decisioni, per seguire gli sviluppi che potrebbero incidere sul loro status. Pertanto, se la Commis- sione europea rileva che il paese terzo, o l'organizzazione internazionale, non soddisfa più le condizioni che giustificano la decisione di adeguatezza, può modificare, sospendere o revocare la decisione. La Commissione può altresì av viare negoziazioni con il paese terzo o l'organiz zazione interna- zionale interessata, per porre rimedio alla situazione alla base della sua decisione.

Le decisioni di adeguatezza adottate dalla Commissione europea in base alla direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sosti- tuite o abrogate da una decisione

della Commissione adottata conformemente alle disposizioni di cui all'articolo 45 del RGPD.

La Commissione ha finora riconosciuto Andorra, Argentina, Canada (organiz- zazioni commerciali che rientrano nell'ambito di applicazione della legge sui dati personali e sui documenti elettronici – PIPEDA), Isole Fær Øer, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera e Uruguay, come forni- tori di una protezione adeguata. Per quanto riguarda i trasferimenti verso gli Stati Uniti, nel 2000 la Commissione europea aveva adottato una decisione di adeguatezza che consentiva trasferimenti alle società che avessero autocerti- ficato la protezione da parte loro dei dati personali trasferiti dall'UE e il rispetto

dei cosiddetti «principi di approdo sicuro»[673]. Tale decisione è stata dichiarata invalida dalla CGUE nel 2015 e nel luglio del 2016 è stata adottata una nuova decisione di adeguatezza, che consente alle società di aderire a partire dal
1° agosto 2016.

Esempio: nella causa *Schrems*[674], il sig. Maximilian Schrems, cittadino austriaco, era stato iscritto a Facebook per diversi anni. I dati forniti dal sig. Schrems a Facebook erano stati trasferiti, in tutto o in parte, dalla controllata irlandese di Facebook verso server situati negli Stati Uniti, dove erano stati trattati. Il sig. Schrems aveva presentato denuncia presso l'autorità di protezione dei dati irlandese, sostenendo che, alla luce delle rivelazioni dell'informatore statunitense Edward Snowden, concernenti le attività di sorveglianza dei servizi di intelligence degli Stati Uniti, il diritto e la prassi vigenti negli Stati Uniti non offrivano una protezione sufficiente dei dati trasferiti verso tale paese. L'autorità irlandese aveva respinto la denuncia a motivo del fatto che, nella sua decisione del 26 luglio 2000, la Commissione aveva ritenuto che, nell'ambito del regime dell'approdo sicuro, gli Stati Uniti garantivano un livello adeguato di protezione dei dati personali trasferiti. La causa era stata portata dinanzi alla High Court irlandese, che l'ha deferita alla CGUE per una pronuncia pregiudiziale.

La CGUE ha dichiarato invalida la decisione della Commissione relativa all’adeguatezza del regime dell’approdo sicuro. La CGUE ha innanzitutto osservato che la decisione consentiva di limitare l’applicabilità dei principi dell’approdo sicuro per la protezione dei dati, al fine di soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia o in base alla legislazione interna degli Stati Uniti. La decisione rendeva pertanto possibili ingerenze nei diritti fondamentali delle persone i cui dati personali erano stati o avrebbero potuto essere trasferiti verso gli Stati Uniti[675]. Essa ha inoltre constatato che la decisione non conteneva alcuna dichiarazione quanto all’esistenza, negli Stati Uniti, di norme destinate a

limitare tali ingerenze o di una tutela giuridica efficace nei confronti delle ingerenze di tale natura[676]. La CGUE ha sottolineato che il livello di protezione dei diritti e delle libertà fondamentali garantito all'interno dell'UE, richiedeva che la normativa comportante un'ingerenza ai sensi degli articoli 7 e 8 prevedesse regole chiare e precise che definissero la portata e l'applicazione di una misura e che imponessero requisiti minimi, deroghe e restrizioni alla protezione dei dati personali[677]. Dal momento che la decisione della Commissione non affermava che gli Stati Uniti garantivano effettivamente tale livello di protezione in considerazione della loro legislazione nazionale o dei loro impegni internazionali, la CGUE ha concluso che essa violava i requisiti della relativa disposizione sui trasferimenti nella direttiva sulla tutela dei dati ed era, pertanto, invalida[678].

Il livello di protezione delle libertà e dei diritti fondamentali non era, pertanto, «sostanzialmente equivalente» a quello garantito dall'UE[679]. La CGUE ha sostenuto che erano stati violati diversi articoli della Carta dei diritti fondamentali dell'UE. In primo luogo, veniva pregiudicato il contenuto essenziale dell'articolo 7, in quanto la legislazione degli Stati Uniti
«consent[iva] alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche». In secondo luogo, vi era stata anche violazione del contenuto essenziale

dell’articolo 47, poiché la normativa non offriva alle persone fisiche rimedi giuridici per quanto riguarda l’accesso ai dati personali, la rettifica o la soppressione di tali dati. Infine, dal momento che l’accordo dell’approdo sicuro violava gli articoli di cui sopra, i dati personali non venivano più trattati in modo lecito, con conseguente violazione dell’articolo 8.

Dopo che la CGUE ha dichiarato invalido l’accordo dell’approdo sicuro, la Com- missione e gli Stati Uniti hanno concordato un nuovo regime, lo scudo UE-USA per la privacy. Il 12 luglio 2016 la Commissione ha adottato una decisione con la quale ha dichiarato che gli Stati Uniti assicurano un livello di protezione

adeguato dei dati personali trasferiti dall'Unione alle organizzazioni statuni- tensi nell'ambito dello scudo per la privacy[680].

Analogamente all'accordo dell'approdo sicuro, il regime dello scudo UE-USA per la privacy mira a proteggere i dati personali che vengono trasferiti dall'UE verso gli Stati Uniti per scopi commerciali[681]. Le aziende statunitensi possono autocertificare volontariamente la loro adesione all'elenco degli aderenti allo scudo, impegnandosi a rispettare le norme in materia di protezione dei dati del quadro normativo. Le competenti autorità statunitensi monitorano e verificano la conformità delle aziende certificate con tali norme.

In particolare, il regime dello scudo per la privacy prevede:

- obblighi di protezione dei dati per le società che ricevono dati personali dall'UE;

- protezione e possibilità di ricorso per le persone, segnatamente la crea- zione di un meccanismo di mediazione che sia indipendente dai servizi di intelligence statunitensi e che tratti i reclami delle persone che ritengono che i loro dati personali siano stati utilizzati in modo illecito dalle autorità statunitensi nel settore della sicurezza nazionale;

- un’analisi annuale comune per monitorare l’attuazione del regime[682]; il primo riesame annuale si è svolto nel settembre 2017[683].

Il governo statunitense ha redatto impegni e garanzie che accompagnano la decisione sullo scudo per la privacy. Questi prevedono limitazioni e garanzie per l'accesso del governo statunitense ai dati personali per finalità di applica- zione della legge e di sicurezza nazionale.

7.3.2. Trasferimenti soggetti a garanzie adeguate

Sia il diritto del CdE sia il diritto dell'UE riconoscono garanzie adeguate fra il titolare del trattamento che trasferisce i dati e il destinatario nel paese terzo o organizzazione internazionale come possibile mezzo per assicurare un livello sufficiente di protezione dei dati per il destinatario.

Nell'ambito del diritto dell'UE, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono consentiti se il titolare del trattamento o il responsabile del trattamento fornisce garanzie adeguate e diritti azionabili, e a condizione che gli interessati dispongano di mezzi di ricorso effettivi[684]. L'elenco di «garanzie adeguate» accettabili è previsto esclusiva- mente nella normativa dell'UE in materia di protezione dei dati. Garanzie ade- guate possono essere stabilite mediante:

- uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;

- norme vincolanti d'impresa;

- clausole tipo di protezione dei dati adottate dalla Commissione europea o da un'autorità di controllo;

- codici di condotta;

- meccanismi di certificazione[685].

Clausole contrattuali personalizzate tra il titolare del trattamento o il respon- sabile del trat tamento nell'UE e il destinatario dei dati in un paese ter zo

costituiscono un altro mezzo per fornire garanzie adeguate. Tali clausole con- trattuali, tuttavia, devono essere autorizzate dall'autorità di controllo compe- tente, prima di poter essere invocate come strumento per il trasferimento di dati personali. Analogamente, le autorità pubbliche possono avvalersi delle disposizioni inserite nei loro accordi amministrativi, a condizione che l'autorità di controllo le abbia autorizzate[686].

Ai sensi del diritto del CdE, i flussi di dati verso uno Stato o un'organizzazione internazionale che non è parte della Convenzione n. 108 modernizzata sono consentiti, a condizione che sia garantito un livello adeguato di protezione. Tale obiettivo può essere raggiunto mediante:

- la legislazione dello Stato o di un'organizzazione internazionale; o

- garanzie ad hoc o standardizzate contenute in un documento giuridica- mente vincolante[687].

Trasferimenti soggetti a clausole contrattuali

Sia il diritto del CdE sia il diritto dell'UE riconoscono le clausole contrattuali sti- pulate fra il titolare del trattamento che trasferisce i dati e il destinatario nel paese terzo come possibile mezzo per garantire un livello sufficiente di prote- zione dei dati per il destinatario[688].

A livello dell’UE, la Commissione europea, con l’ausilio del Gruppo di lavoro articolo 29, ha elaborato clausole tipo per la protezione dei dati, ufficialmente certificate da una decisione della Commissione come prova di un’adeguata protezione dei dati[689]. Poiché le decisioni della Commissione sono vincolanti in ogni loro parte negli Stati membri, le autorità nazionali che controllano i tra- sferimenti dei dati devono riconoscere la validità di tali clausole contrattuali

tipo nei propri procedimenti[690]. Pertanto, se il titolare del trattamento che tra- sferisce i dati e il destinatario nel paese terzo concordano e sottoscrivono tali clausole, l'autorità di controllo dovrebbe avere una prova sufficiente dell'esi- stenza di garanzie adeguate. Tuttavia, nella causa *Schrems*, la CGUE ha stabilito che la Commissione europea non ha la competenza necessaria per limitare i poteri delle autorità nazionali di controllo, di controllare il trasferimento di dati personali verso un paese terzo che è stato oggetto di una decisione di ade- guatezza della Commissione[691]. Pertanto, nulla vieta che le autorità nazionali di controllo esercitino i propri poteri, compreso il potere di sospendere o vie- tare il trasferimento di dati personali, qualora esso avvenga in violazione della normativa europea o nazionale sulla protezione dei dati come, ad esempio, quando l'importatore dei dati non rispetta le clausole contrattuali tipo[692].

L'esistenza di clausole tipo per la protezione dei dati nel quadro giuridico dell'UE non osta a che i titolari del trattamento adottino altre clausole contrat- tuali individuali ad hoc, fatta salva l'autorizzazione dell'autorità di controllo[693]. Essi dovrebbero nondimeno garantire lo stesso livello di protezione previsto dalle clausole tipo per la protezione dei dati. Nell'autorizzare clausole ad hoc, le autorità di controllo devono applicare i meccanismi di coerenza, al fine di garantire un

approccio regolamentare coerente in tutta l'UE[694]. Ciò significa che l'autorità di controllo competente deve comunicare al CEPD il suo progetto di decisione relativo alle clausole. Il CEPD emette un parere sulla questione e l'au- torità di controllo deve tenere tale parere nella massima considerazione nel formulare la propria decisione. Se essa non intende conformarsi al parere del

CEPD, si applica il meccanismo di composizione delle controversie all'interno del CEPD e il comitato adotterà una decisione vincolante[695].

Le caratteristiche più importanti di una clausola contrattuale tipo sono:

- la presenza di una clausola relativa a una terza parte beneficiaria che con- senta agli interessati di esercitare diritti contrattuali anche se non sono parti contraenti del contratto;

- il destinatario o l'importatore dei dati accetta di essere sottoposto all'auto- rità di controllo nazionale del titolare del trattamento che trasferisce i dati e/o dei tribunali in caso di controversia.

Attualmente esistono due serie di clausole tipo per i trasferimenti da titolare del trattamento a titolare del trattamento, fra le quali il titolare del trattamento che trasferisce i dati ha facoltà di scegliere[696]. Per i trasferimenti da titolare del trattamento a responsabile del trattamento esiste un'unica serie di clausole contrattuali tipo.[697] Tuttavia, tali clausole sono attualmente oggetto di procedi- menti giudiziari.

Esempio: dopo che la CGUE ha dichiarato l'invalidità della decisione «approdo sicuro»[698], i trasferimenti di dati personali verso gli Stati Uniti non potevano più

fondarsi su tale decisione di adeguatezza. Mentre i negoziati con le autorità statunitensi erano in corso e in attesa dell'adozione di una nuova

decisione sull'adeguatezza (infine adottata il 12 luglio 2016)[699], i trasferimenti potevano essere effettuati solo nel quadro di altre basi giuridiche, come le clausole contrattuali tipo o le norme vincolanti d'impresa. Diverse società, tra cui Facebook Ireland (nei confronti della quale è stato presentato il caso che ha portato all'annullamento della decisione «approdo sicuro»), sono passate alle clausole contrattuali tipo per continuare i trasferimenti di dati tra l'UE e gli Stati Uniti.

Il sig. Schrems ha presentato una denuncia all'autorità di controllo irlandese, chiedendo la sospensione dei trasferimenti di dati verso gli Stati Uniti sulla base di clausole contrattuali tipo. In sostanza, egli ha sostenuto che, quando i suoi dati personali vengono trasferiti dalla controllata irlandese di Facebook verso Facebook Inc. e verso server situati negli Stati Uniti, non vi è alcuna garanzia di protezione. Facebook Inc. è vincolata da leggi americane che potrebbero obbligarla a divulgare dati personali alle autorità statunitensi preposte all'applicazione della legge e non esiste alcun mezzo di ricorso giurisdizionale a disposizione dei cittadini europei per contestare tale prassi[700]. Per questi motivi, la CGUE ha concluso che la decisione «approdo sicuro» era invalida e, sebbene la sentenza della corte fosse limitata all'esame di tale decisione, il ricorrente ha ritenuto le questioni sollevate pertinenti, quando il trasferimento si basa su clausole contrattuali. Al momento della stesura del presente manuale, il caso

era all’esame della High Court irlandese. Il ricorrente avrebbe l’intenzione di adire la CGUE, per contestare la validità della decisione della Commissione europea sulle clausole contrattuali tipo. Come spiegato nel capitolo 5, solo la CGUE è competente per dichiarare l’invalidità di uno strumento dell’UE.

Trasferimenti soggetti a norme vincolanti d’impresa

Il diritto dell’UE consente anche il trasferimento di dati personali sulla base di norme vincolanti d’impresa per i trasferimenti internazionali che hanno luogo all’interno dello stesso gruppo imprenditoriale o gruppo di imprese che

svolgono un’attività economica comune[701]. Prima di poter utilizzare le norme vincolanti d’impresa come strumento per il trasferimento di dati personali, l’autorità di controllo competente deve approvarle, conformemente alle norme vincolanti d’impresa, avvalendosi del meccanismo di coerenza.

Per essere approvate, le norme vincolanti d’impresa devono essere giuridica- mente vincolanti, includere tutti i principi essenziali in materia di protezione dei dati e applicarsi a tutti i membri del gruppo. Esse devono conferire espres- samente agli interessati diritti azionabili, includere tutti i principi essenziali in materia di protezione dei dati e rispettare determinate prescrizioni for- mali, come l’indicazione della struttura dell’impresa, la descrizione dei tra- sferimenti e le modalità di applicazione dei principi in materia di protezione dei dati. Ciò include la fornitura di tali informazioni agli interessati. Le norme vincolanti d’impresa devono specificare, tra l’altro, i diritti dell’interessato e le disposizioni in materia di responsabilità in caso di violazione delle norme[702]. In sede di approvazione delle norme vincolanti d’impresa, si applica il meccani- smo di coerenza per la cooperazione delle autorità di controllo (descritto nel capitolo 5).

Nell’ambito del meccanismo di coerenza, l’autorità di controllo capofila esa- mina le norme vincolanti d’impresa proposte, adotta un progetto di decisione e lo comunica al CEPD. Il comitato emette un parere

sulla questione e l’autorità di controllo capofila può approvare formalmente le norme vincolanti d’impresa, tenendo in «massima considerazione» il parere del comitato. Tale parere non è giuridicamente vincolante, ma se l’autorità di controllo non intende conformarsi allo stesso, si attua il meccanismo di composizione delle controversie e il comi- tato dev’essere chiamato ad adottare una decisione giuridicamente vincolante, a maggioranza dei due terzi dei suoi membri[703].

Ai sensi del diritto del CdE, le garanzie ad hoc o standardizzate, contenute in un documento giuridicamente vincolante[704], includono anche le norme vincolanti d’impresa.

7.3.3. Deroghe in specifiche situazioni

Nell'ambito del diritto dell'UE, i trasferimenti di dati personali verso un paese terzo possono essere giustificati, anche in mancanza di una decisione o di garanzie adeguate, come le clausole contrattuali tipo o le norme vincolanti d'impresa, in qualsiasi delle seguenti circostanze:

- se l'interessato acconsente esplicitamente al trasferimento dei dati;

- se l'interessato instaura, o si prepara ad instaurare, una relazione contrat- tuale, in cui il trasferimento dei dati all'estero è necessario;

- per concludere un contratto stipulato tra un titolare del trattamento e un terzo a favore dell'interessato;

- per importanti motivi di interesse pubblico;

- per accertare, esercitare o difendere un diritto in sede giudiziaria;

- per tutelare gli interessi vitali dell'interessato;

- per effettuare il trasferimento dei dati a partire da un pubblico registro (si tratta di un caso di interesse prevalente del pubblico generale ad

avere accesso alle informazioni conservate in pubblici registri)[705].

Qualora nessuna di queste condizioni sia applicabile, e qualora i trasferimenti non possano basarsi su una decisione di adeguatezza o su garanzie adeguate, il trasferimento è ammesso soltanto se non è ripetitivo, se riguarda un numero limitato di interessati e se è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano i diritti dell'interessato[706]. In questi casi, il titolare del trattamento deve valutare tutte le circostanze relative al trasferimento e fornire garanzie. Il titolare del tratta- mento deve inoltre informare l'autorità di controllo e gli interessati del trasferi- mento e degli interessi legittimi cogenti che lo giustificano.

Il fatto che le deroghe siano l'ultima risorsa per un trasferimento lecito[707] (alle quali ricorrere solo in mancanza di una decisione di adeguatezza e di altre garanzie) sottolinea la loro natura eccezionale, ed è ulteriormente sottoline- ato nei considerando del RGPD[708]. Come tali, le deroghe sono ammesse come possibilità di «trasferire dati in alcune circostanze» sulla base del consenso e se «il trasferimento è occasionale e necessario»[709] in relazione a un contratto o a un'azione legale.

Inoltre, secondo gli orientamenti del Gruppo di lavoro articolo 29, il ricorso a deroghe in situazioni specifiche dev'essere eccezionale, basato su casi indi- viduali e non può essere utilizzato per trasferimenti massicci o ripetuti[710]. Il Garante europeo della protezione dei dati ha inoltre sottolineato il carattere eccezionale delle deroghe utilizzate come base giuridica per i trasferimenti a norma del regolamento 45/2001, rilevando che tale soluzione dovrebbe essere utilizzata «in casi limitati» e «per i trasferimenti occasionali»[711].

Esempio: una società che fornisce servizi di distribuzione globale (Global Distribution System – GDS), con sede negli Stati Uniti, fornisce il sistema di prenotazioni online per diverse compagnie aeree, alberghi e crociere in tutto il mondo, e tratta

i dati personali di decine di milioni di persone nell'UE. Per trasferire inizialmente i dati verso i suoi server negli Stati Uniti, la società GDS si basa su una deroga come base legittima per i trasferimenti, trattandosi di condizione necessaria per la conclusione di un contratto. Di conseguenza, essa non prevede ulteriori garanzie per i dati personali provenienti dall'Europa, trasferiti verso gli Stati Uniti e in seguito redistribuiti verso alberghi in tutto il mondo (il che significa che non prevede nemmeno garanzie per i trasferimenti successivi). La società GDS non soddisfa i requisiti previsti dal RGPD per i trasferimenti legittimi di dati internazionali, in quanto si basa su una deroga quale motivo legittimo per trasferimenti massicci.

In mancanza di una decisione di adeguatezza, l'UE o i suoi Stati membri pos- sono, per importanti motivi di interesse pubblico, fissare limiti al trasferimento di categorie specifiche di dati personali verso un paese terzo, anche se altre condizioni per tali trasferimenti sono soddisfatte. Questi limiti dovrebbero essere percepiti come eccezionali e gli Stati membri sono tenuti a comunicare alla Commissione le disposizioni pertinenti[712].

Il diritto del CdE consente il trasferimento di dati verso territori che non garan- tiscono una protezione adeguata degli stessi nei casi seguenti:

- se l'interessato ha manifestato il proprio consenso;

- se il trasferimento avviene negli interessi del titolare dei dati;

- se esistono interessi legittimi predominanti previsti per legge, in particolare importanti interessi pubblici;

- se costituisce una misura necessaria e proporzionata in una società democratica[713].

7.3.4. Trasferimenti basati su accordi internazionali

L'UE può concludere accordi internazionali con paesi terzi, per disciplinare il tra- sferimento dei dati

personali per finalità specifiche. Tali accordi devono pre- vedere garanzie adeguate per assicurare la protezione dei dati personali delle persone in questione. Il RGPD lascia impregiudicati tali accordi internazionali[714].

Gli Stati membri possono inoltre concludere accordi internazionali con paesi terzi o organizzazioni internazionali che forniscono un adeguato livello di pro- tezione dei diritti e delle libertà fondamentali delle persone, purché tali accordi non incidano sull'applicazione del RGPD.

Un'analoga disposizione è prevista dall'articolo 12, paragrafo 3, lettera a), della
Convenzione n. 108 modernizzata.

Esempi di accordi internazionali che comportano il trasferimento di dati perso- nali sono costituiti dagli accordi relativi ai codici di prenotazione (PNR).

Codici di prenotazione

I dati relativi ai codici di prenotazione (PNR) sono raccolti dai vettori aerei durante il processo di prenotazione di voli e includono, fra l'altro, nomi, indirizzi, dati delle carte di credito e numeri di posto assegnati dei passeggeri aerei. I vettori aerei raccolgono queste informazioni anche a fini commerciali. L'UE ha concluso accordi con alcuni paesi terzi (Australia, Canada e Stati Uniti) per il tra- sferimento dei dati PNR per prevenire, accertare, indagare e perseguire i reati di terrorismo o reati gravi di natura transnazionale. Inoltre, nel 2016 l'Unione ha adottato la direttiva (UE) 2016/861, nota come direttiva PNR dell'UE[715]. Questa direttiva crea un quadro normativo per gli Stati membri dell'UE, per trasferire i dati PNR alle autorità competenti in altri paesi terzi per prevenire, accertare, indagare o perseguire in modo analogo i reati di terrorismo e altri reati gravi. I trasferimenti di dati PNR alle autorità di paesi terzi sono consentiti caso per caso e sono soggetti a una valutazione individuale per accertare se sono neces- sari per le finalità specificate nella direttiva e a condizione che i diritti fonda- mentali siano rispettati.

Per quanto riguarda gli accordi PNR tra l'UE e i paesi terzi, è stata contestata la loro compatibilità con i diritti fondamentali alla vita privata e alla protezione dei dati sanciti dalla Carta dei diritti fondamentali dell'UE. Quando nel 2014, in seguito ai negoziati con il Canada, l'UE ha firmato un accordo sul trasferimento e sul trattamento dei dati PNR, il Parlamento europeo ha deciso di deferire la questione alla CGUE, affinché valutasse la legalità dell'accordo rispetto al diritto dell'UE, in particolare, con riferimento agli articoli 7 e 8 della Carta.

Esempio: nel suo parere sulla legalità dell'accordo PNR UE-Canada[7 16], la CGUE ha ritenuto che, nella sua forma attuale, l'accordo previsto fosse incompatibile con i diritti fondamentali riconosciuti dalla Carta e, pertanto, non poteva essere concluso. Dal momento che comportava il trattamento di dati personali, esso costituiva un'ingerenza nel diritto alla protezione

dei dati personali tutelato dall'articolo 8 della Carta. Al contempo, esso rappresenta anche una limitazione del diritto al rispetto della vita privata sancito dall'articolo 7, dal momento che, presi nel loro insieme, i dati PNR possono essere aggregati e analizzati in modo da rivelare abitudini di viaggio, relazioni esistenti tra persone diverse, informazioni sulla loro situazione finanziaria, abitudini alimentari e situazione sanitaria, incidendo così sulla loro vita privata.

L'ingerenza nei diritti fondamentali derivante dall'accordo previsto perseguiva un obiettivo di interesse generale, ossia la pubblica sicurezza e la lotta al terrorismo e ai reati gravi di natura transnazionale. Nondimeno, la CGUE ha ricordato che, per essere giustificata, un'ingerenza deve essere limitata allo stretto necessario per conseguire l'obiettivo perseguito. Dopo averne analizzato le disposizioni, la CGUE ha concluso che l'accordo previsto non soddisfaceva il criterio della «stretta necessità». Tra i fattori che la CGUE ha ritenuto di considerare per giungere a tale conclusione vi erano quelli riportati in appresso.

• Il fatto che l'accordo previsto comportava il trasferimento di dati sensibili.
I dati PNR raccolti in base all'accordo previsto potevano comprendere dati sensibili, quali informazioni che rivelano l'origine etnica o razziale, le convinzioni religiose o la salute di un

passeggero. Il trasferimento e il trattamento di dati sensibili da parte delle autorità canadesi poteva presentare un rischio per il principio di non discriminazione e richiedeva, pertanto, una giustificazione precisa e solida, vertente su motivi diversi dalla pubblica sicurezza e la lotta contro i reati gravi. Nell'accordo previsto una siffatta giustificazione mancava[717].

- Anche l'archiviazione continua dei dati PNR di tutti i passeggeri per un periodo di cinque anni, anche dopo la loro partenza dal Canada, è stata ritenuta eccedere i limiti della stretta necessità. La CGUE ha ritenuto ammissibile l'archiviazione, da parte delle autorità canadesi, dei dati di passeggeri rispetto ai quali elementi obiettivi consentono di ritenere che potrebbero presentare, anche dopo la loro partenza dal Canada, un rischio per la sicurezza pubblica. Al contrario, la conservazione dei dati personali di *tutti* i passeggeri con riferimento ai quali non esiste alcuna

prova, nemmeno indiretta, del fatto che presentino un rischio per la sicurezza pubblica, non è giustificata[718].

Il Comitato consultivo della Convenzione n. 108, ha fornito un parere sulle implicazioni della protezione dei dati degli accordi PNR nell'ambito del diritto del CdE[719].

Dati di messaggistica

La Society for Worldwide Interbank Financial Telecommunication (SWIFT), con sede in Belgio, è l'ente responsabile del trattamento della maggior parte dei trasferimenti mondiali di denaro dalle banche europee. La società operava con un «mirror center» negli Stati Uniti e alla stessa era stato richiesto dal diparti- mento del Tesoro statunitense di dare accesso ai dati a fini di indagini sul ter- rorismo, nell'ambito del programma di controllo delle transazioni finanziarie dei terroristi[720].

Dal punto di vista dell'UE, non sussisteva una base giuridica sufficiente per rendere disponibili negli Stati Uniti tali dati, riguardanti soprattutto cittadini dell'UE, solo perché uno dei centri per il trattamento dei dati di SWIFT era ubi- cato negli Stati Uniti.

Nel 2010 è stato concluso un accordo specifico tra l'UE e gli Stati Uniti, noto come accordo SWIFT, volto

a fornire la necessaria base giuridica e a garantire un’adeguata tutela dei dati[721].

Ai sensi dell’accordo, i dati finanziari conservati dalla SWIFT continuano a essere forniti al dipartimento del Tesoro statunitense a fini di prevenzione, indagine, accertamento o azione penale nei confronti del terrorismo o del suo finanziamento. Detto dipartimento può richiedere dati finanziari alla SWIFT, purché la richiesta:

- individui il più chiaramente possibile i dati finanziari;

- motivi espressamente la necessità dei dati;

- sia quanto più possibile precisa onde ridurre al minimo la quantità di dati richiesti;
- non richieda dati relativi all’area unica dei pagamenti in euro (SEPA)[722]. Europol deve ricevere una copia di ciascuna richiesta avanzata dal dipartimento
del Tesoro statunitense e verificare se i principi dell’accordo SWIFT siano rispet-
tati o meno[723]. In caso affermativo, la SWIFT deve fornire i dati finanziari diret- tamente al suddetto dipartimento, che deve conservarli in un ambiente fisico sicuro in cui possano essere consultati solo da analisti che indagano sul terro- rismo o sul relativo finanziamento. I dati finanziari non devono essere collegati con nessun’altra banca dati. In generale, i dati finanziari ricevuti dalla SWIFT devono essere cancellati dopo un periodo massimo di cinque anni successivi alla ricezione degli stessi. I dati finanziari

rilevanti per indagini o procedimenti specifici possono essere conservati solo per tutto il periodo in cui sono neces- sari per tali indagini o procedimenti.

Il dipartimento del Tesoro statunitense può trasferire informazioni estratte dai dati forniti dalla SWIFT a specifiche autorità di contrasto, di pubblica sicurezza o antiterrorismo operanti all'interno o all'esterno degli Stati Uniti solo a fini di pre- venzione, indagine, accertamento o azione penale nei confronti del terrorismo e del suo finanziamento. Se il trasferimento in uscita di dati finanziari interessa un cittadino o una persona residente in uno Stato membro dell'UE, qualsiasi condi- visione dei dati con le autorità di un paese terzo è soggetta al consenso preven- tivo delle autorità competenti dello Stato membro interessato. Possono essere

previste eccezioni nei casi in cui la condivisione dei dati sia essenziale per la prevenzione di una minaccia immediata e grave alla sicurezza pubblica.

Controllori indipendenti, fra cui una persona nominata dalla Commissione euro- pea, monitorano il rispetto dei principi dell'accordo SWIFT. Essi hanno la possibi- lità di controllare in tempo reale e retrospettivamente tutte le ricerche fatte sui dati forniti, il potere di chiedere ulteriori giustificativi in merito al nesso di tale ricerche con il terrorismo, e l'autorità per bloccare qualunque ricerca o la totalità delle ricerche che risulti essere in violazione delle garanzie previste dall'accordo.

Gli interessati hanno il diritto di ottenere conferma dall'autorità di controllo competente dell'UE circa il rispetto dei diritti di tutela dei loro dati personali. Gli interessati hanno anche il diritto di rettifica, cancellazione o blocco del tratta- mento dei propri dati raccolti e conservati dal dipartimento del Tesoro statuni- tense nell'ambito dell'accordo SWIFT. Tuttavia, i diritti di accesso degli interes- sati possono essere soggetti a talune restrizioni giuridiche. Quando l'accesso viene rifiutato, gli interessati devono essere informati per iscritto di tale rifiuto e del loro diritto di ricorrere per via amministrativa e giudiziaria negli Stati Uniti.

L'accordo SWIFT ha una validità quinquennale e il primo periodo di validità è scaduto nell'agosto

2015. Esso è prorogato automaticamente per periodi successivi di un anno, salvo il caso in cui, almeno sei mesi prima, una parte comunichi all’altra la propria intenzione di non prorogare l’accordo. La proroga automatica è stata applicata nell’agosto del 2015, 2016 e 2017 e garantisce la validità dell’accordo SWIFT come minimo fino all’agosto 2018[724].

Al fine di raggiungere un equilibrio fra gli interessi dell'individuo in materia di protezione dei dati e gli interessi della società nella raccolta degli stessi per combattere la criminalità e garantire la sicurezza nazionale e pubblica, il CdE e l'UE hanno adottato specifici strumenti giuridici. Questa sezione fornisce una panoramica del diritto del CdE (sezione 8.1) e del diritto dell'UE (sezione 8.2) sulla protezione dei dati in ambito di polizia e di giustizia penale.

8.1. Il diritto del CdE sulla protezione dei dati in ambito di sicurezza nazionale, polizia e giustizia penale

- La Convenzione n. 108 modernizzata e la raccomandazione del CdE relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza si appli- cano alla protezione dei dati in tutti i settori di attività della polizia.

- La Convenzione sulla criminalità informatica (Convenzione di Budapest) è uno stru- mento giuridico internazionale vincolante che concerne i reati commessi contro o per mezzo delle reti di comunicazione elettronica. Essa è rilevante anche per le indagini riguardanti la criminalità non informatica che coinvolge prove elettroniche.

Un'importante distinzione tra il diritto dell'UE e il diritto del CdE è che quest'ultimo, diversamente dal diritto dell'UE, si applica anche al settore della sicurezza nazion- ale. Questo significa che le parti contraenti devono rientrare nell'ambito di applica- zione dell'articolo 8 della CEDU anche per quanto riguarda le attività connesse alla sicurezza nazionale. Diverse sentenze della Corte EDU riguardano attività statali in settori sensibili della legislazione e della prassi in materia di sicurezza nazionale[725].

Per quanto concerne la polizia e la giustizia penale, a livello europeo la Con- venzione n. 108 modernizzata copre tutti i settori del trattamento dei dati personali e le disposizioni in essa contenute mirano a regolamentare il trat- tamento dei dati personali in generale. Di conseguenza, la Convenzione n. 108 modernizzata si applica alla protezione dei dati nel settore della polizia e della giustizia penale. Il trattamento di dati genetici, dati personali concernenti reati, procedimenti e condanne penali e qualsiasi misura di sicurezza correlata, dati biometrici che identificano in modo univoco una persona nonché eventuali dati personali sensibili, è consentito solo qualora esistano garanzie adeguate alla prevenzione dei rischi che il trattamento di tali dati può comportare per gli interessi, i diritti e le libertà fondamentali dell'interessato, segnatamente il rischio di discriminazione[726]. La raccomandazione è integrata da una guida pratica sull'uso dei dati personali in ambito di polizia, adottata dal Comitato consultivo della Convenzione n. 108[727].

I compiti giuridici delle autorità di polizia e delle autorità giudiziarie penali impongono spesso il trat tamento di dati personali, che può comportare gravi conseguenze per le persone interessate. La raccomandazione relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza, adottata dal CdE nel 1987, contiene orientamenti agli Stati membri del CdE sull'applicazione dei principi della Convenzione n. 108 nel contesto del tratta- mento di dati personali da parte delle autorità di polizia[728].

Esempio: nella causa *D.L. c. Bulgaria*[729], i servizi sociali avevano affidato la ricorrente a un istituto scolastico di custodia in forza di una decisione giudiziaria. Tutta la corrispondenza scritta e le conversazioni telefoniche erano soggette a sorveglianza generalizzata e indiscriminata da parte dell'istituto. La Corte EDU ha ritenuto che vi era stata violazione dell'articolo
8, dal momento che la misura in questione non era necessaria in una società democratica. La Corte ha dichiarato che doveva essere fatto il possibile per consentire ai minori affidati a un istituto di avere contatti sufficienti con il mondo esterno, poiché ciò faceva parte integrante del loro diritto di essere trattati con dignità, ed era assolutamente essenziale per preparare il loro reinserimento nella società. Ciò era applicabile tanto alle visite, quanto alla corrispondenza scritta o alle conversazioni

telefoniche. Inoltre, per quanto riguardava le comunicazioni, la sorveglianza non faceva alcuna distinzione tra i membri della famiglia, le ONG che rappresentano i diritti dei minori o gli avvocati. In aggiunta, la decisione di intercettare le comunicazioni non si basava su un'analisi personalizzata dei rischi nel caso specifico.

Esempio: nella causa *Dragojević c. Croazia*[730], il ricorrente era stato sospettato di coinvolgimento nel traffico di droga. Egli era stato ritenuto colpevole dopo che un giudice istruttore aveva autorizzato l'uso di misure di sorveglianza segreta per intercettare le chiamate telefoniche del ricorrente. La Corte EDU ha ritenuto che la misura, contro la quale era stato presentato ricorso, costituisse un'ingerenza nel diritto al rispetto della vita privata e della corrispondenza. L'autorizzazione data dal giudice istruttore si basava unicamente sull'affermazione delle autorità inquirenti che l'«inchiesta non poteva essere condotta con altri mezzi». La Corte EDU ha altresì notato che

i tribunali penali avevano limitato la loro valutazione sull’uso delle misure di sorveglianza, e che il governo non aveva fornito informazioni sui rimedi a disposizione. Di conseguenza, vi era stata violazione dell’articolo 8.

8.1.1. La raccomandazione relativa alla disciplina dell’uso dei dati personali nell’ambito della pubblica sicurezza

Secondo una giurisprudenza costante della Corte EDU, l’archiviazione e la con- servazione di dati personali da parte della polizia o delle autorità nazionali di pubblica sicurezza costituiscono un’ingerenza ai sensi dell’articolo 8, paragrafo 1, della CEDU. Numerose sentenze della Corte EDU riguardano la giustificazione di tale ingerenza[731].

Esempio: nella causa *B.B. c. Francia*[732], il ricorrente era stato condannato per reati sessuali contro minori di 15 anni, in qualità di persona in posizione di fiducia. Aveva finito di scontare la sua pena nel 2000. Un anno più tardi, aveva chiesto che la menzione di tale sentenza fosse eliminata dal suo casellario giudiziario, ma la sua richiesta era stata respinta. Nel 2004, una legge francese ha creato una banca dati giudiziaria nazionale di autori di reati sessuali e il ricorrente è stato informato del suo inserimento nella stessa. La Corte EDU ha statuito che l’inserimento in una banca dati giudiziaria

nazionale di una persona condannata per reati sessuali rientrava nell'ambito di applicazione dell'articolo 8 della CEDU. Tuttavia, poiché erano state attuate garanzie sufficienti per la protezione dei dati, fra cui il diritto dell'interessato di richiedere la cancellazione dei dati, la durata limitata della conservazione dei dati e l'accesso limitato agli stessi, era stato raggiunto un giusto equilibrio fra gli opposti interessi privati e pubblici in questione. La Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

Esempio: nella causa *S. e Marper c. Regno Unito*[733], entrambi i ricorrenti erano stati accusati di aver commesso reati, ma non erano stati condannati.

Tuttavia, le impronte digitali, i campioni di cellule e i profili del DNA dei ricorrenti erano custoditi e conservati dalla polizia. La conservazione a tempo indeterminato dei suddetti dati biometrici era autorizzata per legge qualora una persona fosse sospettata di aver commesso un reato, anche se la stessa veniva successivamente assolta o prosciolta. La Corte EDU ha statuito che la conservazione generale e indiscriminata di dati personali, illimitata nel tempo e nel cui ambito le persone assolte avevano solo limitate possibilità di richiedere la cancellazione, costituiva un'ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Una questione fondamentale nel contesto delle comunicazioni elettroniche è l'ingerenza delle autorità pubbliche nei diritti alla vita privata e alla protezione dei dati. I mezzi di sorveglianza o di intercettazione delle comunicazioni, come i dispositivi di ascolto o intercettazione, sono consentiti solo se sono previsti dalla legge e costituiscono una misura necessaria in una società democratica nell'interesse:

- della sicurezza nazionale;
- della sicurezza pubblica;
- degli interessi monetari dello Stato;

- della repressione di reati o

- della protezione dell'interessato o dei diritti e delle libertà altrui.

Molte altre sentenze della Corte EDU riguardano la giustificazione dell'ingerenza nel diritto alla vita privata mediante sorveglianza.

Esempio: nella causa *Allan c. Regno Unito*[734], le autorità avevano registrato in segreto le conversazioni private tra un detenuto e un amico nella sala visite del carcere e con un codetenuto in una cella. La Corte EDU ha statuito che l'uso di dispositivi di audioregistrazione e videoregistrazione nella cella del ricorrente, nella sala visite del carcere e su un codetenuto costituisse un'ingerenza nel diritto del ricorrente alla vita privata. Poiché nel momento in

cui si erano verificati i fatti non esisteva un sistema legale per regolamentare l'uso di dispositivi di registrazione in segreto da parte della polizia, detta ingerenza non era conforme alla legge. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Esempio: nella causa *Roman Zakharov c. Russia*[735], il ricorrente aveva intentato un procedimento giudiziario contro tre operatori di reti mobili. Egli aveva sostenuto che il suo diritto alla riservatezza delle comunicazioni telefoniche era stato violato, in quanto gli operatori avevano installato apparecchiature che consentivano al Servizio federale di sicurezza di intercettare le sue comunicazioni telefoniche senza previa autorizzazione giudiziaria. La Corte EDU ha ritenuto che le disposizioni giuridiche nazionali che disciplinano l'intercettazione delle comunicazioni non offrivano garanzie adeguate ed efficaci contro l'arbitrarietà e il rischio di abuso. In particolare, la legislazione nazionale non prevedeva la cancellazione dei dati memorizzati una volta perseguita la finalità della conservazione. Inoltre, malgrado fosse richiesta un'autorizzazione giudiziaria, il controllo giurisdizionale aveva portata limitata.

Esempio: nella causa *Szabó e Vissy c. Ungheria*[736], i ricorrenti asserivano che la legislazione ungherese violava l'articolo 8 della CEDU, in quanto non era sufficientemente dettagliata o precisa. Essi avevano

inoltre sostenuto che la legislazione non forniva garanzie sufficienti contro l’abuso e l’arbitrarietà. La Corte EDU ha dichiarato che il diritto ungherese non prevedeva che la sorveglianza fosse assoggettata all’autorizzazione di un tribunale. Tuttavia, la Corte ha osservato che, sebbene subordinata all’autorizzazione del ministro della giustizia, tale sorveglianza era eminentemente di carattere politico e non poteva garantire la prevista valutazione della «stretta necessità». Inoltre, il diritto nazionale non prevedeva un controllo giurisdizionale, dal momento che agli interessati non sarebbe stata inviata alcuna notifica. La Corte ha concluso asserendo l’esistenza di una violazione dell’articolo 8 della CEDU.

Poiché il trattamento di dati personali da parte delle autorità di polizia può avere conseguenze rilevanti per gli interessati, sono particolarmente neces- sarie norme dettagliate sulla protezione dei dati ai fini del trattamento dei dati personali in questo settore. La raccomandazione del CdE relativa alla disciplina

dell’uso dei dati personali nell’ambito della pubblica sicurezza ha cercato di affrontare la questione fornendo orientamenti sulle modalità di raccolta dei dati personali per le attività di polizia; sulle modalità di tenuta degli archivi di dati in questo settore e sulle persone che dovrebbero essere autorizzate ad accedere a tali archivi, comprese le condizioni per il trasferimento dei dati ad autorità di polizia straniere; sulle modalità di esercizio dei diritti alla protezione dei dati da parte degli interessati e sulle modalità di attuazione del controllo da parte di autorità indipendenti. Anche l’obbligo di garantire un’adeguata sicurezza dei dati era stato considerato.

La raccomandazione non consente una raccolta illimitata e indiscriminata di dati da parte delle autorità di polizia, ma limita la raccolta di dati personali da parte di dette autorità a quanto necessario per la prevenzione di un pericolo concreto o per la repressione di un reato specifico. Ogni ulteriore raccolta di dati dovrebbe basarsi su una legislazione nazionale specifica. Il trattamento di dati sensibili dovrebbe essere limitato allo stretto necessario nel contesto di una particolare indagine.

Quando i dati personali sono raccolti all’insaputa dell’interessato, quest’ultimo deve esserne informato non appena la divulgazione dei dati non arrechi più pregiudizio alle indagini. La raccolta di dati attraverso dispositivi tecnici di sor- veglianza o

altri mezzi automatizzati deve avere una base giuridica specifica.

Esempio: nella causa *Versini-Campinchi e Crasnianski c. Francia*[737], la ricorrente, un avvocato, aveva avuto una conversazione telefonica con un cliente, la cui linea telefonica veniva intercettata su richiesta di un giudice istruttore. La trascrizione della conversazione mostrava che aveva rivelato informazioni coperte dal segreto professionale. Il pubblico ministero aveva inviato tali informazioni all'ordine degli avvocati, che aveva inflitto un'ammenda alla ricorrente. La Corte EDU ha riconosciuto l'esistenza di un'ingerenza nel diritto al rispetto della vita privata e della corrispondenza, non solo della persona il cui telefono era stato intercettato, ma anche della ricorrente la cui comunicazione era stata intercettata e trascritta. L'ingerenza era conforme alla legge e perseguiva l'obiettivo legittimo della prevenzione di disordini. La ricorrente aveva ottenuto un riesame della legittimità della presentazione della trascrizione delle registrazioni telefoniche nel contesto del procedimento disciplinare intentato contro di lei. Anche se la ricorrente non aveva avuto la possibilità di chiedere l'annullamento della trascrizione

della conversazione telefonica, la Corte EDU ha ritenuto che vi era stato un controllo efficace, in grado di limitare l'ingerenza contestata a quanto necessario in una società democratica. La Corte EDU ha affermato che l'argomento secondo cui la possibilità di intentare un procedimento penale contro un avvocato sulla base della trascrizione potrebbe avere un effetto dissuasivo sulla libertà di comunicazione tra un avvocato e il suo cliente, e quindi sui diritti di difesa di quest'ultimo, non era credibile se la divulgazione da parte dell'avvocato stesso poteva equivalere a una condotta illegale da parte dello stesso. Di conseguenza, non è stata riscontrata una violazione dell'articolo 8 della CEDU.

La raccomandazione del CdE relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza stabilisce che, all'atto di conservare dati personali, deve essere operata una chiara distinzione tra i dati amministrativi e i dati di polizia; i dati personali di diverse categorie di interessati, quali sospet- tati, detenuti, vittime e testimoni; e fra i dati basati sui fatti reali e quelli basati su sospetti o deduzioni.

I dati acquisiti dalla polizia devono essere strettamente limitati nello scopo, cosa che incide sulla comunicazione di tali dati a terzi: il trasferimento o la comunicazione di tali dati in ambito di polizia dovrebbero essere regolamen- tati

in base alla presenza o meno di un interesse legittimo alla condivisione delle informazioni. Il trasferimento o la comunicazione di tali dati al di fuori dell'ambito di polizia dovrebbero essere consentiti solo qualora sussistano chi- ari obblighi o autorizzazioni legali.

Esempio: nella causa *Karabeyoğlu c. Turchia*[7 38], le linee telefoniche del ricorrente, un giudice, erano state messe sotto controllo nell'ambito di un'indagine penale concernente un'organizzazione illegale alla quale era sospettato di appartenere o alla quale si riteneva fornisse assistenza e supporto. A seguito della decisione di non luogo a procedere, il pubblico ministero incaricato dell'indagine penale aveva distrutto le registrazioni in questione. Tuttavia, una copia era rimasta in possesso degli investigatori giudiziari, i quali avevano successivamente utilizzato il materiale pertinente nell'ambito di un'indagine disciplinare nei confronti del ricorrente. La Corte EDU ha dichiarato che la normativa pertinente era stata violata, in quanto le informazioni erano state utilizzate per finalità diverse da quelle per cui erano state raccolte e non erano state distrutte entro il termine previsto per

legge. L'ingerenza nel diritto del ricorrente al rispetto della vita privata non era conforme alla legge per quanto riguardava il procedimento disciplinare nei suoi confronti.

Il trasferimento o la comunicazione a livello internazionale dovrebbero essere limitati alle autorità di polizia straniere ed essere basati su disposizioni giuridi- che specifiche, possibilmente accordi internazionali, a meno che non siano nec- essari per prevenire un pericolo grave e imminente.

Il trattamento di dati personali da parte della polizia deve essere oggetto di un con- trollo indipendente per garantire il rispetto della normativa nazionale in materia di protezione dei dati. Gli interessati devono godere di tutti i diritti di accesso sanciti dalla Convenzione n. 108 modernizzata. Se i diritti di accesso degli interessati sono stati limitati in applicazione dell'articolo 9 della Convenzione n. 108 nell'interesse di specifiche indagini di polizia e del perseguimento di reati, la normativa nazionale deve garantire all'interessato il diritto di ricorrere all'autorità di controllo nazionale competente per la protezione dei dati o a un altro organo indipendente.

8.1.2. La Convenzione di Budapest sulla criminalità informatica

Poiché le attività criminali si avvalgono sempre più dei sistemi elettronici di trattamento dei dati e comportano conseguenze per gli stessi, per affrontare tale sfida sono necessarie nuove disposizioni giuridiche in ambito penale. Il CdE, pertanto, ha adottato uno strumento giuridico internazionale, la Convenzi- one sulla criminalità informatica – nota anche come Convenzione di Budapest – per affrontare la questione dei crimini commessi contro e per mezzo delle reti elettroniche[739]. La suddetta Convenzione è aperta all'adesione anche degli Stati non membri del CdE. Nel 2018, quattordici Stati non membri del CdE[740] erano parti contraenti della convenzione e altri sette paesi non membri l'avevano fir- mata o erano stati invitati ad aderirvi.

La Convenzione sulla criminalità informatica resta il trattato internazionale più autorevole in materia di violazioni di diritto commesse su Internet o altre reti

informatiche. Essa impone alle parti di aggiornare e di armonizzare le rispet- tive leggi penali contro la pirateria e altre violazioni della sicurezza, fra cui la violazione del diritto d'autore, la frode informatica, la pedopornografia e altre attività informatiche illecite. La convenzione prevede inoltre poteri proce- durali che riguardano la ricerca sulle reti informatiche e l'intercettazione delle comunicazioni nel contesto della lotta contro la criminalità informatica. Infine, essa rende possibile un'effettiva cooperazione internazionale. Un protocollo addizionale alla Convenzione riguarda l'incriminazione di atti di propaganda di natura razzista e xenofoba sulle reti informatiche.

Benché non sia uno strumento volto a promuovere la protezione dei dati, la con- venzione considera alla stregua di reati attività che potrebbero violare i diritti dell'interessato alla protezione dei propri dati. Essa impone inoltre alle parti contraenti di adottare misure legislative che consentano alle rispettive autorità nazionali di intercettare i dati relativi al traffico e ai contenuti[741]. Essa obbliga inoltre le parti contraenti, in sede di attuazione della Convenzione, a prevedere un'adeguata protezione dei diritti umani e delle libertà, compresi i diritti sanciti dalla CEDU, come il diritto alla protezione dei dati[742]. Per aderire alla Convenzione di Budapest sulla criminalità informatica, le parti contraenti non devono obbliga- toriamente aderire anche alla Convenzione n. 108.

8.2. Il diritto dell’UE sulla protezione dei dati in ambito di polizia e di giustizia penale

- All’interno dell’UE, la protezione dei dati in ambito di polizia e di giustizia penale è regolamentata nel contesto del trattamento nazionale e transfrontaliero da parte delle autorità di polizia e delle autorità giudiziarie degli Stati membri e degli operatori dell’UE.

- A livello degli Stati membri, la direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali deve essere trasposta nella legislazione nazionale.

- La protezione dei dati nel settore della cooperazione transfrontaliera in materia di polizia e applicazione della legge, segnatamente nella lotta contro il terrorismo e la criminalità transfrontaliera, è disciplinata da strumenti giuridici specifici.

- Esistono norme specifiche sulla protezione dei dati per l’Agenzia dell’Unione europea per la cooperazione nell’attività di contrasto (Europol), l’Unità europea di cooperazione giudiziaria (Eurojust) e la neocostituita Procura europea, organismi dell’Unione che sostengono e promuovono l’applicazione della legge a livello transfrontaliero.

- Esistono norme specifiche sulla protezione dei dati anche per i sistemi d’informazione comune istituiti a livello dell’UE per gli scambi transfrontalieri di informazioni fra le autorità di polizia e giudiziarie competenti. Esempi impor- tanti sono costituiti dal sistema d’informazione Schengen II (SIS II), dal sistema di informazione visti (VIS) e da Eurodac, un sistema centralizzato contenente i dati relativi alle impronte digitali di cittadini di paesi terzi e apolidi che presentano domanda di asilo in uno degli Stati membri dell’UE.

- L’UE sta aggiornando le disposizioni in materia di protezione dei dati di cui sopra, per conformarsi alle disposizioni della direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali.

8.2.1. La direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali

La direttiva 2016/680/UE relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati (la direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali)[743] è volta a proteggere i dati personali raccolti e trattati per finalità di giustizia penale, quali:

- la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

- l'esecuzione di una sanzione penale, e

- nei casi in cui la polizia o altre autorità incaricate dell'applicazione della legge si adoperano per salvaguardare la legalità e ai fini della salvaguardia

contro e la prevenzione di minacce alla sicurezza pubblica e ai diritti fonda- mentali della società, che potrebbero costituire reato.

La direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudi- ziarie penali tutela i dati personali relativi a diverse categorie di interessati coinvolti in procedimenti penali, quali testimoni, persone informate dei fatti, vittime, indiziati e complici. Le autorità di polizia e le autorità giudiziarie penali sono tenute a rispettare le disposizioni della direttiva quando trattano tali dati per finalità di applicazione della legge, nell'ambito di applicazione sia personale che materiale della direttiva[744].

Tuttavia, l'utilizzo dei dati per una finalità diversa è consentito anche a deter- minate condizioni. Il trattamento dei dati per una finalità di applicazione della legge diversa da quella per cui sono raccolti è consentito solo se legittimo, nec- essario e proporzionato conformemente al diritto nazionale o dell'UE[745]. Per altre finalità si applicano le norme del regolamento generale sulla protezione dei dati. La registrazione e la documentazione della condivisione dei dati cos- tituiscono uno degli obblighi specifici delle autorità competenti al fine di con- tribuire a chiarire le responsabilità in seguito a denunce.

Le autorità competenti che operano nel settore della polizia e della giustizia penale sono autorità

pubbliche o autorità incaricate dal diritto nazionale e dotate di poteri pubblici per esercitare le funzioni di autorità pubblica[746], ad esempio, carceri gestite privatamente[747]. L'applicabilità della direttiva si estende sia al trat- tamento dei dati a livello nazionale e al trattamento in ambito transfrontaliero tra polizia e autorità giudiziarie degli Stati membri sia ai trasferimenti internazi- onali da parte delle autorità competenti verso paesi terzi e organizzazioni inter- nazionali[748]. Non si applica alla sicurezza nazionale né al trattamento dei dati per- sonali da parte di istituzioni, organi, uffici e agenzie dell'UE[749].

La direttiva si basa, in larga misura, sui principi e sulle definizioni contenuti nel regolamento generale sulla protezione dei dati, tenendo conto della specificità dei settori della polizia e della giustizia penale. Il controllo può essere effettuato dalle stesse autorità degli Stati membri che lo esercitano ai sensi del regola- mento generale sulla protezione dei dati. La designazione di responsabili della protezione dei dati e l'effettuazione di valutazioni d'impatto sulla protezione dei dati sono state introdotte nella direttiva come nuovi obblighi per le autorità di polizia e giudiziarie in campo penale[750]. Sebbene tali concetti si ispirino al regola- mento generale sulla protezione dei dati, la direttiva riguarda la natura specifica delle autorità di polizia e delle autorità giudiziarie penali. Rispetto al trattamento dei dati a fini commerciali, che è disciplinato dal regolamento, il trattamento di dati connesso alla sicurezza può richiedere un certo livello di flessibilità. Per esempio, garantire agli interessati lo stesso livello di protezione in termini di diritto di informazione, accesso o cancellazione dei propri dati personali ai sensi del regolamento generale sulla protezione dei dati potrebbe significare che qual- siasi operazione di controllo effettuata a fini di contrasto diventerebbe inefficace nel contesto dell'applicazione della legge. La direttiva non contiene, pertanto, il principio di trasparenza. In modo analogo, è necessario che anche i principi della minimizzazione dei dati e della limitazione della finalità, che impongono di limitare i dati personali solo a quanto necessario rispetto alle

finalità per le quali sono trattati e che siano trattati per finalità legittime e specifiche, ven- gano applicati in modo flessibile nei trattamenti di dati relativi alla sicurezza. Le informazioni raccolte e conservate dalle autorità competenti per un caso specif- ico, possono rivelarsi estremamente utili per la risoluzione di casi futuri.

Principi relativi al trattamento di dati personali

La direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudi- ziarie penali stabilisce alcune garanzie fondamentali per quanto riguarda l'uso dei dati personali. Essa precisa inoltre i principi che guidano il trattamento di tali dati. Gli Stati membri devono far sì che i dati personali siano:

- trattati in modo lecito e corretto;

- raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità;

- adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati;

- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti ris- petto alle finalità per le quali sono trattati;

- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

- trattati in modo da assicurare un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeg- uate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzi- one o dal danno accidentali[751].

Ai sensi della direttiva, il trattamento è lecito solo nella misura in cui sia necessario per l'esecuzione del compito pertinente. Inoltre, esso dovrebbe essere effettuato da un'autorità competente nel perseguimento delle finalità specificate nella diret- tiva e basarsi sul diritto dell'UE o nazionale[752]. I dati non devono essere conservati più a lungo di quanto necessario e devono essere cancellati o esaminati periodica- mente entro termini prestabiliti. Devono essere utilizzati solo da un'autorità com- petente e per le finalità per le quali sono stati raccolti, trasmessi o resi disponibili.

Diritti dell’interessato

La direttiva stabilisce inoltre i diritti dell’interessato. Essi comprendono:

• Il diritto di ricevere informazioni. Gli Stati membri devono obbligare il tito- lare del trattamento a mettere a disposizione dell’interessato 1) l’identità e i dati di contatto del titolare del trattamento, 2) i dati di contatto del responsabile della protezione dei dati, 3) le finalità del trattamento pre- visto, 4) il diritto di proporre reclamo a un’autorità di controllo e i dati di contatto della stessa e 5) il diritto di accesso, rettifica o cancellazione dei dati personali e di limitare il trattamento degli stessi[753]. In aggiunta a questi obblighi generali di informazione, la direttiva stabilisce che, in casi specifici e per consentire l’esercizio dei loro diritti, i titolari del trattamento devono fornire agli interessati informazioni sulla base giuridica per il trattamento e sulla durata di conservazione dei dati. Se i dati personali devono essere

trasmessi ad altri destinatari, anche in paesi terzi o presso organizzazioni internazionali, gli interessati devono essere informati circa le categorie di tali destinatari. Infine, i titolari del trattamento devono fornire ogni ulte- riore informazione, tenendo conto delle circostanze specifiche in cui i dati vengono trattati, ad esempio qualora i dati siano stati raccolti in sede di sorveglianza discreta, ossia senza che l'interessato ne fosse a conoscenza. Ciò garantisce un trattamento corretto dei dati dell'interessato[754].

- Il diritto di accesso ai dati personali. Gli Stati membri devono garantire che l'interessato abbia il diritto di sapere se sia o meno in corso un trattamento dei suoi dati personali. In tal caso, l'interessato dovrebbe avere accesso a determinate informazioni, quali le categorie di dati personali trattati[755]. Tut- tavia, tale diritto può essere limitato, ad esempio, al fine di non comprom- ettere indagini o il perseguimento di un reato, o per proteggere la sicurezza pubblica e i diritti e le libertà altrui[756].

- Il diritto di rettifica dei dati personali. Gli Stati membri sono tenuti a gar- antire che l'interessato possa, senza ingiustificato ritardo, ottenere la retti- fica di dati personali inesatti. Inoltre, l'interessato ha anche il diritto di otte- nere l'integrazione dei dati personali incompleti[757].

• Il diritto alla cancellazione dei dati personali e alla limitazione del tratta- mento. In alcuni casi, il titolare del trattamento deve cancellare i dati per- sonali. Inoltre, l'interessato può ottenere la cancellazione dei propri dati personali, ma solo se sono trattati illecitamente[758]. In talune situazioni, il trat- tamento dei dati personali può essere limitato, anziché cancellato. Ciò può verificarsi quando 1) l'esattezza dei dati personali è contestata ma non può essere accertata o 2) quando i dati personali sono necessari a fini probatori[759].

Se il titolare del trattamento rifiuta la rettifica o la cancellazione dei dati person- ali, o la limitazione del trattamento dei dati, l'interessato deve esserne infor- mato per iscritto. Gli Stati membri possono limitare tale diritto all'informazione,

fra l'altro, per proteggere la sicurezza pubblica o i diritti e le libertà altrui, per gli stessi motivi previsti per la limitazione del diritto di accesso[760].

Di norma, l'interessato ha il diritto di ottenere informazioni sul trattamento dei suoi dati personali e gode del diritto di accesso, rettifica o cancellazione della limitazione del trattamento, che può esercitare direttamente presso il titolare del trattamento. Come alternativa, l'esercizio indiretto dei diritti dell'interessato attraverso l'autorità di controllo per la protezione dei dati competente è possibile anche nel quadro della direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, e diventa effettivo quando il titolare del trattamento limita il diritto dell'interessato[761]. L'articolo 17 della direttiva prevede che gli Stati membri adottino misure volte a gar- antire che i diritti degli interessati possano essere esercitati anche attraverso l'autorità di controllo competente. Per questo motivo, il titolare del trattamento deve informare l'interessato della possibilità di un accesso indiretto.

Obblighi del titolare del trattamento e del responsabile del trattamento

Nell'ambito della direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, i titolari del trattamento sono le autorità pubbliche

competenti o altri organismi dotati di pertinenti poteri pubblici e autorità pub- blica, che determinano le finalità e i mezzi del trattamento di dati personali. La direttiva stabilisce diversi obblighi per i titolari del trattamento, al fine di garantire un elevato livello di protezione per i dati personali trattati ai fini dell'applicazione della legge.

Le autorità competenti devono tenere un registro delle operazioni di tratta- mento che effettuano nei sistemi di trattamento automatizzato. Le regis- trazioni devono essere conservate almeno per la raccolta, la modifica, la con- sultazione, la comunicazione, compresi i trasferimenti, l'interconnessione e la cancellazione dei dati personali[762]. La direttiva stabilisce che le registrazi- oni delle consultazioni e delle comunicazioni devono consentire di stabilire la data e l'ora di tali operazioni, la motivazione e, nella misura del possibile, l'identificazione della persona che ha consultato il sistema o comunicato i

dati personali, e i destinatari dei dati personali in questione. Le registrazioni devono essere usate ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali[763]. Su richiesta dell'autorità di controllo, il titolare del trattamento e il responsabile del trattamento devono mettere le registrazioni a disposizione della stessa.

In particolare, i titolari del trattamento hanno un obbligo generale di attuare misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato ai sensi della direttiva, ed essere in grado di dimostrare la liceità di tale trattamento[764]. Nell'elaborare tali misure, essi devono tenere conto della natura, dell'ambito di applicazione, del contesto del trattamento e, soprat- tutto, dei potenziali rischi per i diritti e le libertà delle persone. I titolari del trattamento dovrebbero adottare politiche interne e attuare misure che agev- olino la conformità ai principi della protezione dei dati, segnatamente il prin- cipio di protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita[765]. Quando un trattamento può presentare un rischio elevato per i diritti delle persone – a causa, per esempio, dell'uso di nuove tecnologie – i titolari del trattamento devono effettuare una valutazione dell'impatto sulla protezione dei dati, prima di procedere al

trattamento[766]. La direttiva elenca anche le misure che i titolari del trattamento devono mettere in atto per garantire la sicurezza del trattamento. Esse includono misure volte a impedire l'accesso non autorizzato ai dati personali trattati, garantire che le persone autorizzate abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione, che le funzioni del sistema di trattamento siano operative e che i dati personali conservati non possano essere falsati da un errore di funziona- mento del sistema[767]. In caso di violazione dei dati personali, i titolari del trat- tamento devono notificare l'autorità di controllo entro tre giorni, descrivendo la natura della violazione, le probabili conseguenze, le categorie dei dati personali in questione e il numero approssimativo dei rispettivi interessati. La violazione dei dati personali deve inoltre essere comunicata all'interessato «senza ingi- ustificato ritardo», quando è suscettibile di presentare un rischio elevato per i diritti e le libertà dello stesso[768].

La direttiva contiene il principio di responsabilizzazione, che impone ai titolari del trattamento l'obbligo di mettere in atto misure che garantiscano il rispetto di tale principio. I titolari del trattamento devono tenere un registro di tutte le categorie di attività di trattamento sotto la loro responsabilità: il contenuto dettagliato di tali registrazioni è specificato nell'articolo 24 della direttiva. Su richiesta, i registri devono essere messi a disposizione delle autorità di con- trollo per consentire loro il monitoraggio delle operazioni di trattamento del titolare del trattamento. Un'altra importante misura per rafforzare la respon- sabilità è la designazione di un responsabile della protezione dei dati (RPD). I titolari del trattamento devono designare un RPD, sebbene la direttiva con- senta agli Stati membri di esentare da tale obbligo le autorità giurisdizionali e le altre autorità giudiziarie indipendenti[769]. I compiti del RPD sono simili a quelli previsti dal regolamento generale sulla protezione dei dati. Il RPD sorveglia l'osservanza della direttiva e fornisce informazioni e consulenza ai dipendenti che effettuano il trattamento per adempiere agli obblighi previsti dalla leg- islazione in materia di protezione dei dati. Il RPD emette inoltre pareri in merito alla necessità di effettuare una valutazione d'impatto sulla protezione dei dati e funge da punto di contatto per l'autorità di controllo.

Trasferimenti verso paesi terzi o organizzazioni internazionali

Analogamente al regolamento generale sulla protezione dei dati, la direttiva stabilisce le condizioni per il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali. Se i dati personali fossero trasmessi liberamente al di fuori della giurisdizione dell'UE, le garanzie e l'efficace protezione previste dalla legislazione dell'UE potrebbero essere compromesse. Tuttavia, le condizioni sono molto diverse da quelle del regolamento generale sulla protezione dei dati. Il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali è consentito se[770]:

- il trasferimento è necessario per le finalità della direttiva;

- i dati personali sono trasferiti a un'autorità competente, ai sensi della direttiva, del paese terzo o dell'organizzazione internazionale, sebbene esista una deroga a tale norma in casi singoli e specifici[771].

- il trasferimento verso paesi terzi o organizzazioni internazionali di dati personali ricevuti nell’ambito della cooperazione transfrontaliera richiede l’autorizzazione dello Stato membro dal quale i dati provengono, anche se sono previste deroghe in casi urgenti;

- la Commissione europea ha adottato una decisione di adeguatezza, sono state previste garanzie adeguate o si applica la deroga per i trasferimenti in situazioni specifiche;

- i trasferimenti successivi di dati personali verso un altro paese terzo o un’altra organizzazione internazionale richiedono l’autorizzazione prelimin- are dell’autorità che ha effettuato il trasferimento, la quale tiene conto, tra l’altro, della gravità del reato e del livello di protezione dei dati personali nel paese di destinazione del secondo trasferimento internazionale[772].

Ai sensi della direttiva, i trasferimenti di dati personali possono aver luogo se una di tre condizioni è soddisfatta. La prima richiede che la Commissione europea abbia emesso una decisione di adeguatezza ai sensi della direttiva. La decisione può essere applicabile all’intero territorio di un paese terzo, a settori specifici di un paese terzo o a un’organizzazione internazionale. Tuttavia, ciò è possibile solo se è garantito un livello di protezione

adeguato e se le condizioni definite nella direttiva sono soddisfatte[773]. In tali casi, il trasferimento di dati personali non è soggetto all'autorizzazione dello Stato membro[774]. La Commis- sione europea deve controllare gli sviluppi che potrebbero incidere sul funzi- onamento delle decisioni di adeguatezza. Inoltre, la decisione deve includere un meccanismo di riesame periodico. La Commissione può altresì revocare, modificare o sospendere una decisione, qualora dalle informazioni disponibili risulti che le condizioni all'interno del paese terzo o dell'organizzazione inter- nazionale non garantiscano più un livello di protezione adeguato. In tal caso, la Commissione deve avviare consultazioni con il paese terzo o l'organizzazione internazionale per cercare di porre rimedio alla situazione.

In mancanza di una decisione d'adeguatezza, i trasferimenti possono essere effettuati sulla base di garanzie adeguate. Essi possono essere previsti in uno strumento giuridicamente vincolante, oppure il titolare del trattamento può

effettuare un'autovalutazione delle circostanze relative al trasferimento dei dati personali e concludere per l'esistenza di garanzie adeguate. L'autovalutazione dovrebbe tenere conto di eventuali accordi di cooperazione conclusi tra Europol o Eurojust e il paese terzo o l'organizzazione internazionale, dell'esistenza di obblighi di riservatezza, della limitazione di finalità nonché delle garanzie for- nite che i dati non saranno utilizzati per qualsiasi forma di trattamento crudele e disumano, inclusa la pena di morte[775]. In quest'ultimo caso, il titolare del trat- tamento è tenuto a informare l'autorità di controllo competente in merito alle categorie di trasferimenti nell'ambito di questa categoria[776].

In mancanza di una decisione di adeguatezza o di garanzie adeguate, i tras- ferimenti possono comunque essere consentiti in situazioni specifiche delin- eate nella direttiva. Essi includono, tra l'altro, la tutela degli interessi vitali dell'interessato o di un'altra persona e la prevenzione di una minaccia grave e immediata alla sicurezza pubblica dello Stato membro o di un paese terzo[777].

In casi singoli e specifici, i trasferimenti da parte di autorità competenti verso destinatari stabiliti in paesi terzi che non siano autorità competenti sono con- sentiti, oltre che in presenza delle tre condizioni sopra menzionate, se sono soddisfatte anche ulteriori condizioni previste dall'articolo 39

della diret- tiva. In particolare, il trasferimento deve essere strettamente necessario per l'assolvimento di un compito dell'autorità competente che opera il trasferi- mento, la quale deve altresì determinare che nessun diritto o nessuna libertà fondamentale degli interessati prevalga sull'interesse pubblico che giustifica il trasferimento. Tali trasferimenti devono essere documentati e l'autorità competente che opera il trasferimento deve informare l'autorità di controllo competente[778].

Infine, per quanto riguarda i paesi terzi e le organizzazioni internazionali, la direttiva prescrive anche lo sviluppo di meccanismi di cooperazione internazi- onale per facilitare l'applicazione efficace della legislazione, contribuendo così ad assistere le autorità di controllo per la protezione dei dati nella cooperazione con le loro controparti all'estero[779].

Controllo indipendente e mezzi di ricorso per gli interessati

Ogni Stato membro deve garantire che una o più autorità nazionali di controllo indipendenti siano incaricate di fornire consulenza e sorvegliare l'applicazione delle disposizioni adottate ai sensi della direttiva[780]. L'autorità di controllo isti- tuita ai fini della direttiva può essere la stessa autorità di controllo istituita dal regolamento generale sulla protezione dei dati, ma gli Stati membri sono liberi di designare un'autorità diversa, purché soddisfi i criteri di indipendenza. Inol- tre, chiunque può rivolgersi alle autorità di controllo con un'istanza relativa alla tutela dei propri diritti e delle libertà personali per quanto riguarda il tratta- mento dei dati personali da parte delle autorità competenti.

Quando l'esercizio dei diritti dell'interessato è negato per motivi preminenti, l'interessato deve avere il diritto di ricorrere alla competente autorità di controllo nazi- onale e/o di adire l'autorità giudiziaria. Chiunque subisca un danno cagionato da una violazione del diritto nazionale di attuazione della direttiva, ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o da qualsiasi altra autorità com- petente in base al diritto dello Stato membro[781]. In generale, gli interessati devono avere il diritto di accesso a mezzi di ricorso giurisdizionali per qualsiasi violazione dei loro diritti garantiti dalla

legislazione nazionale di attuazione della direttiva[782].

8.3. Altri strumenti giuridici specifici in materia di protezione dei dati nell'ambito dell'applicazione della legge

Oltre alla direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, lo scambio di informazioni tra gli Stati membri in settori specifici è disciplinato da una serie di strumenti giuridici, quali la decisione quadro 2009/315/GAI del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudizi- ario, la decisione 2000/642/GAI del Consiglio concernente le modalità di coop- erazione tra le unità di informazione finanziaria degli Stati membri per quanto riguarda lo scambio di informazioni e la decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di

informazioni e intelligence tra le autorità degli Stati membri dell'Unione euro- pea incaricate dell'applicazione della legge[783].

Occorre evidenziare che la cooperazione transfrontaliera[784] fra le autorità competenti implica uno scambio sempre più intenso di dati sull'immigrazione. Questa sfera del diritto non è considerata par te del settore della pubblica sicurezza e della giustizia penale ma, sotto diversi aspetti, è rilevante per l'attività della polizia e delle autorità giudiziarie. Lo stesso dicasi per i dati relativi alle merci importate nell'UE o da questa esportate. L'eliminazione dei con- trolli di frontiera interna nell'area Schengen ha determinato un aumento del rischio di frodi, costringendo gli Stati membri a intensificare la cooperazione, in particolare rafforzando lo scambio transfrontaliero di informazioni, per accer- tare e perseguire in modo più efficace le violazioni del diritto doganale nazionale e dell'UE. Inoltre, negli ultimi anni il mondo ha visto aumentare forme gravi di criminalità organizzata e terrorismo, che possono coinvolgere i viaggi inter- nazionali e, in molti casi, ha evidenziato la necessità di una maggiore cooper- azione transfrontaliera tra le forze di polizia e le autorità di contrasto[785].

La decisione di Prüm

Un importante esempio di cooperazione tran sfrontaliera istituzionaliz- zata mediante lo scambio di dati tenuti a livello nazionale è la decisione
2008/615/GAI del Consiglio, con le relative disposizioni di attuazione nella decisione 2008/615/GAI, sul potenziamento della cooperazione transfron- taliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (decisione di Prüm), che nel 2008 ha integrato nel diritto dell'UE il trattato di

Prüm[786]. Il trattato di Prüm era un accordo internazionale di cooperazione di polizia firmato nel 2005 da Austria, Belgio, Francia, Germania, Lussemburgo, Paesi Bassi e Spagna[787].

Lo scopo della decisione di Prüm è quello di agevolare agli Stati membri fir- matari il compito di migliorare la condivisione delle informazioni ai fini della prevenzione e della lotta contro la criminalità in tre settori: terrorismo, crimi- nalità transfrontaliera e migrazione illegale. A tal fine, la decisione contiene disposizioni per quanto riguarda:

- l'accesso automatizzato a profili DNA, ai dati relativi alle impronte digitali e a taluni dati nazionali di immatricolazione dei veicoli;

- la trasmissione dei dati in relazione a eventi di rilievo a dimensione transfrontaliera;

- la trasmissione delle informazioni per prevenire reati terroristici;

- altre misure per potenziare la cooperazione di polizia transfrontaliera.

Le banche dati messe a disposizione nell'ambito della decisione di Prüm sono regolamentate interamente dalla normativa nazionale, ma lo scambio di dati è disciplinato ulteriormente dalla stessa decisione, la cui compatibilità con la diret- tiva

sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali dovrà essere oggetto di valutazione. Gli organi competenti per il controllo di tali flussi di dati sono le autorità nazionali di controllo per la protezione dei dati.

Decisione quadro 2006/960/GAI – l'iniziativa svedese

La decisione quadro 2006/960/GAI (iniziativa svedese)[788] rappresenta un altro esempio di cooperazione transfrontaliera per quanto riguarda lo scambio di

dati detenuti a livello nazionale dalle autorità di contrasto. L'iniziativa svedese riguarda specificamente lo scambio di intelligence e informazioni e prevede norme specifiche in materia di protezione dei dati di cui all'articolo 8.

In base a questo strumento, l'uso delle informazioni e dell'intelligence scambi- ate deve essere soggetto alle disposizioni nazionali in materia di protezione dei dati dello Stato membro ricevente, sulla base delle stesse norme che sarebbero state applicate se fossero state raccolte in detto Stato membro. L'articolo 8 va oltre stabilendo che, nel fornire le informazioni e l'intelligence, l'autorità com- petente incaricata dell'applicazione della legge può imporre condizioni ai sensi della legislazione nazionale, per il loro utilizzo da parte dell'autorità compe- tente incaricata dell'applicazione della legge che le riceve. Tali condizioni pos- sono altresì essere applicabili alla comunicazione dei risultati dell'indagine penale o dell'operazione di intelligence criminale nell'ambito delle quali era avvenuto lo scambio di informazioni e intelligence. Tuttavia, quando la leg- islazione nazionale prevede deroghe alle restrizioni di utilizzazione (ad esem- pio, a favore di autorità giudiziarie, istituzioni legislative, ecc.), le informazioni e l'intelligence possono essere utilizzate solo previa consultazione con lo Stato membro che trasmette i dati.

Le informazioni e l'intelligence forniti possono essere utilizzati:

- per gli scopi per i quali sono stati forniti o

- per la prevenzione di un pericolo grave e immediato per la sicurez za pubblica.

Il trattamento per scopi diversi può essere consentito, ma soltanto previa autorizzazione dello Stato membro che trasmette i dati.

L'iniziativa svedese prevede inoltre che i dati personali trattati siano protetti conformemente a strumenti internazionali quali:

- la convenzione del Consiglio d'Europa sulla protezione delle persone ris- petto al trattamento automatizzato di dati a carattere personale[789];

- il protocollo addizionale di detta Convenzione dell’8 novembre 2001 con- cernente le autorità di controllo ed i flussi transfrontalieri[790];

- la raccomandazione n. R(87) 15 del Consiglio d’Europa relativa alla disci- plina dell’uso dei dati personali nell’ambito della pubblica sicurezza[791].

La direttiva UE-PNR

I dati del codice di prenotazione (PNR) si riferiscono alle informazioni sui passeggeri del trasporto aereo raccolte dai vettori e da essi conservate a fini commerciali nei loro sistemi di prenotazione e di controllo delle partenze. Tali dati contengono diversi tipi di informazioni, come le date di viaggio, l’itinerario, i dati relativi al biglietto, i recapiti, l’agenzia di viaggi presso la quale il viag- gio è stato prenotato, le modalità di pagamento, il posto assegnato e le car- atteristiche dei bagagli[792]. Il trattamento dei dati PNR può aiutare le autorità preposte all’applicazione della legge a identificare indagati noti o persone potenzialmente sospette ed effettuare valutazioni basate sui tipi di sposta- mento e altri indicatori tipicamente associati alle attività criminali. L’analisi dei dati PNR consente anche il controllo retrospettivo delle rotte più usate e dei contatti delle persone sospettate di essere coinvolte in attività criminali, che possono permettere alle autorità di contrasto di identificare reti

criminali[793]. Come spiegato nella sezione 7, l'UE ha concluso alcuni accordi con paesi terzi per lo scambio dei dati PNR. Inoltre, ha introdotto il trattamento dei dati PNR all'interno dell'UE, attraverso la direttiva 2016/681/UE sull'uso dei dati PNR a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (direttiva PNR dell'UE)[794]. Questa diret-

tiva prevede l'obbligo per i vettori aerei di trasmettere i dati PNR alle autorità competenti e stabilisce rigorose garanzie di protezione dei dati per il trat- tamento e la raccolta degli stessi. La direttiva PNR dell'UE si applica ai voli internazionali da e verso l'UE, ma anche ai voli intra-UE se uno Stato membro decide in tal senso[795].

I dati PNR raccolti devono contenere solo le informazioni consentite dalla direttiva PNR dell'UE. Essi devono essere conservati in un'unica unità d'informazione, all'interno di un luogo sicuro nel territorio di ciascuno Stato membro. I dati PNR devono essere resi anonimi sei mesi dopo la loro tras- missione da parte del vettore aereo e conservati per un periodo massimo di cinque anni[796]. I dati PNR vengono scambiati tra gli Stati membri, tra gli Stati membri ed Europol e con paesi terzi, ma unicamente caso per caso.

La trasmissione e il trattamento dei dati PNR e i diritti salvaguardati per gli interessati devono essere in linea con la direttiva sulla protezione dei dati des- tinata alla polizia e alle autorità giudiziarie penali e devono garantire l'elevato livello di protezione della vita privata e dei dati personali previsto dalla Carta, dalla Convenzione n. 108 modernizzata e dalla CEDU.

Le autorità nazionali di controllo indipendenti competenti ai sensi della diret- tiva sulla protezione

dei dati destinata alla polizia e alle autorità giudiziarie penali sono altresì incaricate di dare consulenza in merito alle disposizioni adottate dagli Stati membri ai sensi della direttiva PNR dell'UE e di sorvegliarne l'applicazione.

Conservazione dei dati relativi alle telecomunicazioni

La direttiva sulla conservazione dei dati[797], dichiarata invalida l'8 aprile 2014 nella sentenza *Digital Rights Ireland*, obbligava i fornitori di servizi di comuni- cazione a tenere a disposizione i metadati, con il fine specifico di repressione di reati gravi, per un periodo di almeno sei mesi, ma non superiore a 24 mesi,

indipendentemente dal fatto che il fornitore avesse ancora necessità di con- servare tali dati a fini di fatturazione o di fornitura tecnica del servizio.

La conservazione di dati relativi alle telecomunicazioni interferisce chiara- mente con il diritto alla protezione dei dati[798]. Il fatto che tale ingerenza sia giustificata o meno è stato contestato in diversi procedimenti giudiziari negli Stati membri dell'UE[799].

Esempio: nella causa *Digital Rights Ireland* e *Kärntner Landesregierung e a.*[800], il gruppo Digital Rights e il sig. Seitlinger avevano presentato dinanzi alla High Court (Alta corte) in Irlanda e alla corte costituzionale in Austria, rispettivamente, un ricorso con cui mettevano in discussione la legittimità di misure nazionali che consentono la conservazione di dati relativi a comunicazioni elettroniche. La Digital Rights aveva chiesto alla Court irlandese di dichiarare la nullità della direttiva 2006/24 e della parte della legge nazionale sulla giustizia penale relativa agli atti terroristici. In modo analogo, il sig. Seitlinger e oltre 11 000 altri ricorrenti avevano contestato e chiesto l'annullamento di una disposizione della legislazione austriaca sulle telecomunicazioni che attuava la direttiva 2006/24.

Nell'esaminare tali richieste di pronuncia pregiudiziale, la CGUE ha dichiarato invalida la

direttiva sulla conservazione dei dati. Secondo la CGUE, i dati che potevano essere conservati ai sensi della direttiva, presi nel loro complesso, fornivano informazioni precise riguardo alle persone. Inoltre, la CGUE ha esaminato la gravità dell'ingerenza nei diritti fondamentali del rispetto della vita privata e della protezione dei dati personali. Essa ha constatato che la conservazione risponde a un obiettivo di interesse pubblico, segnatamente la lotta contro la criminalità grave e, di conseguenza, la sicurezza pubblica. Nondimeno, la CGUE ha dichiarato che, adottando la direttiva, il legislatore dell'UE aveva violato il principio di proporzionalità. Sebbene la direttiva possa essere considerata adeguata ai fini del perseguimento del suo obiettivo,

«l’ingerenza vasta e particolarmente grave di tale direttiva nei diritti fondamentali in parola non è sufficientemente regolamentata in modo da essere effettivamente limitata allo stretto necessario».

In assenza di una legislazione specifica, la conservazione dei dati è consen- tita come misura preventiva in deroga alla riservatezza dei dati relativi alle telecomunicazioni ai sensi della direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche)[801], ma deve essere finalizzata unicamente alla lotta contro le forme gravi di criminalità. Tale conservazione deve essere limitata a quanto strettamente necessario per quanto riguarda le categorie di dati conservati, i mezzi di comunicazione interessati, le persone coinvolte e la durata scelta per la conservazione. Le autorità nazionali possono avere accesso ai dati conservati nel rispetto di condizioni rigorose, compreso il controllo preliminare da parte di un’autorità indipendente. I dati devono essere conservati all’interno del territorio dell’UE.

Esempio: in seguito alla sentenza *Digital Rights Ireland* e *Kärntner Landesregierung e a.*[802], altri due casi sono stati presentati dinanzi alla CGUE in relazione all’obbligo generale di conservare i dati delle telecomunicazioni, imposto in Svezia e nel Regno Unito ai fornitori di servizi di comunicazione

elettronica, come richiesto dalla direttiva sulla conservazione dei dati invalidata. Nella causa *Tele2 Sverige* e *Home Department c. Tom Watson e a.*[803], la CGUE ha decretato che una legislazione nazionale che prevede la conservazione generalizzata e indifferenziata dei dati, senza richiedere alcuna correlazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica, e che non specifica alcuna condizione (ad esempio, la durata della conservazione, la zona geografica, le cerchie di persone suscettibili di essere implicate in un reato grave), travalica i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, come richiede la direttiva 2002/58/CE, letta alla luce della Carta dei diritti fondamentali dell'UE.

Prospettiva

Nel gennaio 2017, la Commissione europea ha pubblicato una proposta di regolamento relativo al rispetto della vita privata e alla tutela dei dati person- ali nelle comunicazioni elettroniche, inteso ad abrogare e sostituire la diret- tiva 2002/58/CE[804]. La proposta non contiene disposizioni specifiche sulla conservazione dei dati. Tuttavia, essa prevede che gli Stati membri possano limitare per legge alcuni obblighi e diritti previsti dal regolamento, qualora tale restrizione costituisca una misura necessaria e proporzionata per la sal- vaguardia di specifici interessi pubblici, compresa la sicurezza nazionale, la difesa, la sicurezza pubblica nonché la prevenzione, l'indagine, l'accertamento o il perseguimento dei reati o l'esecuzione di sanzioni penali[805]. Pertanto, gli Stati membri potrebbero mantenere o creare quadri di riferimento nazionali in materia di conser vazione dei dati, che prevedano misure di conser vazi- one mirate, nella misura in cui tali quadri siano conformi al diritto dell'Unione, tenendo conto della giurisprudenza della CGUE sull'interpretazione della diret- tiva e-privacy e della Carta dei diritti fondamentali dell'UE[806]. Al momento della stesura di questo manuale, le discussioni sull'attuazione del regolamento erano in corso.

Accordo quadro UE-USA sulla protezione dei dati personali scambiati a fini di contrasto

Il 1° febbraio 2017, è entrato in vigore l'accordo quadro UE-USA stipulato con gli Stati Uniti sul trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento dei reati penali[807]. L'accordo quadro UE-USA mira a garantire un livello elevato di protezione dei dati per i cittadini dell'UE, rafforzando nel contempo la cooperazione tra le autorità di contrasto dell'UE e degli Stati Uniti. Esso integra gli accordi UE-USA e Stati membri-USA in vigore

tra le autorità preposte all'applicazione della legge, contribuendo al tempo stesso a stabilire norme chiare e armonizzate sulla protezione dei dati per i futuri accordi in questo settore. In tal senso, l'accordo mira a istituire un quadro giuridico duraturo per facilitare lo scambio d'informazioni.

L'accordo non fornisce di per sé una base giuridica adeguata per lo scambio di dati personali, ma prevede piuttosto adeguate garanzie di protezione dei dati per le persone interessate. Esso disciplina tutti i casi di trattamento di dati per- sonali necessario per prevenire, indagare, accertare e perseguire reati, com- preso il terrorismo[808].

L'accordo prevede molteplici strumenti di salvaguardia per garantire che i dati personali siano utilizzati esclusivamente per gli scopi specificati nell'accordo stesso. In particolare, fornisce ai cittadini dell'UE la seguente tutela:

• limitazioni all'uso dei dati: i dati personali possono essere utilizzati solo ai fini di prevenzione, indagine, accertamento e perseguimento di reati;

• protezione contro una discriminazione arbitraria o ingiustificata;

• trasferimenti successivi: per qualsiasi trasferimento successivo verso un paese al di fuori degli Stati Uniti o dell'UE oppure verso

un’organizzazione internazionale occorre il previo consenso dell’autorità competente del paese che ha effettuato il trasferimento di dati originario;

- qualità dei dati: i dati personali devono essere conservati tenendo conto della loro esattezza, pertinenza, tempestività e completezza;

- sicurez za del trat tamento, compresa la notifica delle violazioni di dati personali;

- il trattamento di dati sensibili è consentito solo in presenza di garanzie ade- guate conformi alla legge;

- periodi di conservazione: i dati personali non possono essere conservati più a lungo di quanto sia necessario e appropriato;

- diritti di accesso e rettifica: ogni persona ha il diritto di accedere ai propri dati personali, a determinate condizioni, e di chiederne la rettifica qualora siano inesatti;

- le decisioni automatizzate richiedono garanzie adeguate, compresa la pos- sibilità di ottenere l'intervento umano;

- supervisione efficace, inclusa la cooperazione tra le autorità di supervisione dell'UE e statunitensi, e

- ricorso giurisdizionale ed esecutività: i cittadini dell'UE hanno il diritto[809] di adire i tribunali statunitensi nei casi in cui le autorità statunitensi neghino l'accesso o la rettifica o divulghino illegalmente i loro dati personali.

Nell'ambito dell'«accordo quadro» è stato inoltre istituito un sistema per noti- ficare eventuali violazioni della protezione dei dati all'autorità di controllo competente dello Stato membro delle persone interessate, ove necessario. Le garanzie giuridiche previste dall'accordo garantiscono la parità di trattamento dei cittadini dell'UE negli Stati Uniti in caso di violazione della vita privata[810].

8.3.1. Protezione dei dati nell’ambito delle autorità giudiziarie e di polizia dell’UE

Europol

Europol, l’agenzia dell’UE preposta alla attività di contrasto, ha sede centrale a L’Aia e dispone di unità nazionali Europol (UNE) in ciascuno Stato membro.

Europol è stato istituito nel 1998; il suo attuale status giuridico come istituzione dell'UE è basato sul regolamento che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (regolamento Europol)[811]. Il man- dato di Europol è quello di sostenere le attività di prevenzione e d'indagine sulla criminalità organizzata, sul terrorismo e su altre forme gravi di criminal- ità, elencate nell'allegato I al regolamento Europol, che interessino due o più Stati membri. Esso espleta la sua funzione attraverso lo scambio di informazi- oni, agendo in tal senso come piattaforma centrale dell'UE per lo scambio di informazioni, e fornisce analisi dell'intelligence e valutazioni della minaccia.

Per conseguire i propri obiettivi, Europol ha creato il sistema d'informazione Europol, che mette a disposizione degli Stati membri una banca dati per lo scambio di informazioni e intelligence in materia penale attraverso le rispet- tive UNE. Il sistema d'informazione Europol può essere usato per rendere dis- ponibili dati che riguardino persone sospettate di aver commesso un reato di competenza di Europol o che sono state condannate per un siffatto reato o persone riguardo alle quali vi siano indicazioni concrete per ritenere che pos- sano commettere tali reati. Europol e le UNE possono inserire dati direttamente nel sistema d'informazione Europol ed estrarli dallo stesso. Solo la parte che ha inserito i dati nel

sistema può modificarli, rettificarli o cancellarli. Anche gli organismi dell'UE, i paesi terzi e le organizzazioni internazionali possono fornire informazioni a Europol.

Europol può ottenere informazioni, compresi i dati personali, anche da fonti accessibili al pubblico, come Internet. I trasferimenti di dati personali a organ- ismi dell'UE sono consentiti soltanto se necessario per lo svolgimento dei com- piti di Europol o dell'organismo dell'UE destinatario. I trasferimenti di dati per- sonali verso paesi terzi o organizzazioni internazionali sono consentiti solo se la Commissione europea decide che il paese o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato («decisione di ade- guatezza»), o sulla base di un accordo internazionale o di un accordo di coop- erazione. Europol può ricevere e trattare i dati personali provenienti da parti private e persone private solo in presenza delle rigide condizioni che preve- dono che tali dati siano trasferiti attraverso una UNE conformemente al diritto nazionale, un punto di contatto di un paese terzo o di un'organizzazione inter- nazionale con i quali esiste una cooperazione istituita sulla base di un accordo

di cooperazione o un’autorità di un paese terzo o un’organizzazione interna- zionale che forma oggetto di una decisione di adeguatezza o con cui l’UE ha concluso un accordo internazionale. Tutti gli scambi di informazioni sono effet- tuati attraverso un’applicazione di rete per lo scambio di informazioni protetta (*Secure Information Exchange Network Application* – SIENA).

In risposta a nuovi sviluppi, sono stati istituiti centri specializzati in seno a Europol. Il Centro europeo per la lotta alla criminalità informatica è stato isti- tuito presso Europol nel 2013[812]. Esso funge da piattaforma centrale dell’UE per lo scambio di informazioni sulla criminalità informatica, contribuendo a velociz- zare le risposte in caso di reati on-line, sviluppando e mobilitando capacità di analisi tecnica forense digitale e delineando le migliori pratiche sulle indagini concernenti la criminalità informatica. Il Centro si focalizza su reati informatici:

• commessi da gruppi organizzati per generare ingenti profitti da attività criminali come la frode online;

• che recano gravi danni alla vittima, come lo sfruttamento sessuale dei minori online;

• che colpiscono i sistemi d’informazione o le infrastrutture critiche all’interno dell’UE.

Nel gennaio 2016 è stato creato il centro europeo antiterrorismo (*European Counter Terrorism Centre* – ECTC), per fornire un supporto operativo agli Stati membri nelle indagini connesse a reati terroristici. Esso effettua controlli incro- ciati sui dati operativi intempo reale rispetto ai dati già acquisiti da Europol, portando rapidamente alla luce gli elementi finanziari, e analizza tutti i dettagli investigativi disponibili, per contribuire alla creazione di un quadro strutturato di una rete terroristica[813].

Il Centro europeo per la lotta al traffico di migranti (*European Migrant Smug- gling Centre* – EMSC) è stato istituito nel febbraio 2016 a seguito di una riun- ione del Consiglio tenutasi nel novembre 2015, per sostenere gli Stati membri

nel combattere e smantellare le reti criminali coinvolte nel traffico di migranti. Esso funge da piattaforma centrale per lo scambio di informazioni a sostegno degli uffici della task force regionale dell'UE a Catania (Italia) e al Pireo (Gre- cia), che assistono le autorità nazionali in diversi settori, tra cui la condivisione di intelligence, indagini penali e il perseguimento di reti dedite alla tratta di essere umani[814].

Il regime di protezione dei dati che disciplina le attività di Europol è raffor- zato e ispirato dai principi del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE[815] ed è inoltre coerente con la direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, la Convenzione n. 108 modernizzata e la raccomandazione relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza.

È consentito il trattamento di dati personali relativi a vittime di reato, testi- moni o altre persone che possono fornire informazioni riguardanti reati e a persone di età inferiore agli anni diciotto se strettamente necessario e propor- zionato per prevenire o combattere forme di criminalità rientranti negli obiet- tivi di Europol[816]. Il trattamento di dati personali sensibili è vietato, salvo se strettamente necessario e proporzionato per prevenire o combattere forme di criminalità rientranti negli obiettivi di Europol e se tali dati

integrano altri dati personali trattati da Europol[817].
In entrambi i casi solo Europol ha accesso ai dati pertinenti[818].

La conservazione dei dati è consentita solo per un periodo di tempo necessario e proporzionato e la sua continuazione è soggetta ad un esame ogni tre anni in assenza del quale i dati sono automaticamente cancellati[819].

In determinate circostanze, Europol può trasferire direttamente i dati personali a un organismo dell'UE, a un'autorità di un paese terzo o a un'organizzazione

internazionale[820]. La violazione di dati personali suscettibile di ledere i diritti e le libertà dell'interessato, deve essere loro comunicata senza ingiustificato ritardo[821]. A livello di Stato membro, un'autorità nazionale di controllo è desig- nata al fine di vigilare sul trattamento dei dati personali effettuato da Europol[822].

Il GEPD ha il compito di sorvegliare e assicurare la tutela dei diritti e delle lib- ertà fondamentali delle persone fisiche con riguardo al trattamento di dati per- sonali da parte di Europol e di fornire a Europol e agli interessati pareri su tutte le questioni relative al trattamento dei dati personali. A tal fine, il GEPD agisce in qualità di organismo che gestisce le indagini e i reclami e agisce in stretta cooperazione con le autorità nazionali di controllo[823]. Il GEPD e le autorità nazionali di controllo si riuniscono almeno due volte all'anno nel consiglio di cooperazione, che ha funzione consultiva[824]. Gli Stati membri sono tenuti a des- ignare per legge un'autorità di controllo incaricata di vigilare affinché il trasferi- mento, il reperimento e la comunicazione a Europol di dati personali da parte dello Stato membro interessato avvengano in modo lecito[825]. Gli Stati mem- bri sono inoltre tenuti a garantire che l'autorità nazionale di controllo possa agire in modo del tutto indipendente nello svolgimento dei suoi compiti e nell'esercizio delle sue funzioni ai sensi del regolamento Europol[826]. Ai fini della verifica

della liceità del trattamento dei dati, del controllo interno delle proprie attività e per garantire l'integrità e la sicurezza dei dati, Europol registra o doc- umenta le proprie attività di trattamento dei dati. I registri devono contenere informazioni sulle operazioni di trattamento nei sistemi di trattamento autom- atizzato relative alla raccolta, la modifica, la consultazione, la comunicazione, la combinazione e la cancellazione[827].

I ricorsi avverso le decisioni del GEPD possono essere proposte dinanzi alla CGUE[828]. La persona fisica che subisca un danno cagionato da un trattamento illecito dei dati ha il diritto di ottenere il risarcimento del danno da Europol o dallo Stato membro responsabile, proponendo azione dinanzi alla CGUE nel

primo caso o dinanzi all'autorità nazionale competente nel secondo caso[829]. Inoltre, un gruppo specializzato di controllo parlamentare congiunto costituito dai parlamenti nazionali e dal Parlamento europeo può controllare le attività di Europol[830]. Ogni persona ha diritto di accesso a qualsiasi dato personale che Europol possa detenere sul suo conto, oltre al diritto di richiedere che tali dati personali siano controllati, rettificati o cancellati. Tali diritti possono essere sog- getti a deroghe e limitazioni.

Eurojust

Eurojust, istituito nel 2002, è un organismo dell'UE con sede a L'Aia. Esso promuove la cooperazione giudiziaria nell'ambito di indagini e azioni penali in merito a gravi forme di criminalità che interessino almeno due Stati membri[831]. Eurojust ha il compito di:

- stimolare e migliorare il coordinamento delle indagini e delle azioni penali tra le autorità nazionali competenti dei vari Stati membri;

- agevolare l'esecuzione di richieste e decisioni relative alla cooperazione giudiziaria.

Le funzioni dell'Eurojust sono esercitate dai membri nazionali. Ogni Stato mem- bro delega un giudice o un pubblico ministero presso l'Eurojust, il cui status è soggetto alla legge nazionale ed è dotato delle

competenze necessarie per svolgere i compiti necessari a stimolare e migliorare la cooperazione giudizi- aria. Inoltre, i membri nazionali agiscono congiuntamente come collegio per svolgere compiti speciali nell'ambito del mandato dell'Eurojust.

L'Eurojust può trattare dati personali nella misura necessaria a conseguire i propri obiettivi. Ciò si limita, tuttavia, al trattamento di specifiche informazioni

concernenti persone sospettate di aver commesso, partecipato o essere state condannate per un reato che rientra nella sfera di competenza dell'Eurojust. L'Eurojust può anche trattare talune informazioni concernenti testimoni o vit- time di reati sottoposti alla propria competenza[832]. In casi eccezionali e per un periodo di tempo limitato, l'Eurojust può trattare dati personali più ampi relativi alle circostanze di un reato qualora detti dati abbiano rilievo immediato per le indagini in corso. Nell'ambito della propria competenza, l'Eurojust può coop- erare con altre istituzioni, organismi e agenzie dell'UE e scambiare con questi dati personali. L'Eurojust può anche cooperare e scambiare dati personali con paesi terzi e altre organizzazioni.

Con riguardo alla protezione dei dati, l'Eurojust deve garantire un livello di pro- tezione almeno equivalente a quello garantito dai principi di cui alla Conven- zione n. 108 modernizzata e successive modifiche. Nei casi di scambio di dati, occorre osservare norme e restrizioni specifiche attuate in un accordo di coop- erazione o in un accordo operativo, conformemente alle decisioni del Consiglio sull'Eurojust e alle disposizioni del regolamento interno dell'Eurojust relative al trattamento e alla protezione dei dati personali[833].

In seno all'Eurojust è stata istituita un'autorità di controllo comune indip- endente con il compito di monitorare il trattamento dei dati personali da parte

dell'Eurojust. Le persone possono rivolgersi all'autorità di controllo se non sono soddisfatte della decisione dell'Eurojust a una richiesta di accesso, rettifica, blocco del trattamento o cancellazione di dati personali. In caso di trattamento illecito di dati personali, l'Eurojust, conformemente al diritto nazionale dello Stato membro in cui ha sede, ossia i Paesi Bassi, è responsabile di qualsiasi pregiudizio cagionato all'interessato.

Prospettiva

Nel luglio 2013 la Commissione europea ha presentato una proposta di regola- mento per riformare l'Eurojust. Questa proposta era accompagnata da una proposta relativa all'istituzione di una Procura europea (cfr. infra). Questo regolamento mira ad ottimizzare le funzioni e la struttura ai fini della con- formità con il trattato di Lisbona. Inoltre, l'obiettivo della riforma è operare una

chiara divisione tra i compiti operativi dell’Eurojust, svolti dal collegio, e i suoi compiti amministrativi. Ciò consentirà anche agli Stati membri di concentrarsi maggiormente sui compiti operativi. Sarà istituito un nuovo comitato esecutivo, per assistere il collegio nello svolgimento dei compiti amministrativi[834].

Procura europea

Gli Stati membri hanno competenza esclusiva per perseguire i reati di frode e di applicazione impropria del bilancio dell’UE, che hanno anche potenziali implicazioni transfrontaliere. L’importanza di individuare, perseguire e inviare a giudizio gli autori di tali reati è aumentata, specialmente in considerazione dell’attuale crisi economica[835]. La Commissione europea ha proposto un regola- mento relativo all’istituzione di una Procura europea (EPPO) indipendente[836], con l’obiettivo di combattere i reati che ledono gli interessi finanziari dell’UE. La Procura europea sarà istituita mediante la procedura di cooperazione raffor- zata, che permette ad un minimo di nove Stati membri di instaurare una coop- erazione rafforzata in un settore nell’ambito di strutture dell’UE, senza coin- volgere altri paesi[837]. Belgio, Bulgaria, Croazia, Cipro, Estonia, Finlandia, Francia, Germania, Grecia, Lettonia, Lituania, Lussemburgo, Portogallo, Repubblica ceca, Romania, Slovenia, Slovacchia e Spagna hanno

aderito alla cooperazione raf- forzata; l'Austria e l'Italia hanno espresso l'intenzione di aderirvi[838].

L'EPPO sarà competente per le indagini e la repressione delle frodi nell'UE e altri reati lesivi degli interessi finanziari dell'UE, allo scopo di coordinare in modo efficiente le indagini e le azioni penali nei diversi ordinamenti giuridici nazionali e migliorare l'uso di risorse e lo scambio di informazioni a livello europeo[839].

L'EPPO sarà posta sotto l'autorità del procuratore europeo, con la presenza di almeno un procuratore europeo delegato avente sede in ciascuno Stato mem- bro, incaricato delle indagini e delle azioni penali in tale Stato membro.

La proposta prevede solide garanzie a salvaguardia dei diritti delle persone coinvolte nelle indagini dell'EPPO, come previsto dalla legislazione nazion- ale, dal diritto dell'UE e dalla Carta dei diritti fondamentali dell'UE. Le misure investigative riguardanti soprattutto i diritti fondamentali saranno soggette alla previa autorizzazione di un organo giurisdizionale nazionale[840]. Le indagini dell'EPPO saranno soggette a controllo giurisdizionale da parte delle autorità giurisdizionali nazionali[841].

Al trat tamento dei dati personali amministrativi da par te dell 'EPPO sarà applicabile il regolamento sulla protezione dei dati da parte delle istituzioni dell'UE[842]. Per il trattamento dei dati personali relativo a questioni operative, come Europol, l'EPPO avrà un regime di protezione dei dati autonomo, simile a quello che disciplina le attività di Europol e dell'Eurojust, dal momento che l'esercizio delle funzioni dell'EPPO coinvolgerà il trattamento dei dati personali con le autorità preposte all'applicazione della legge e all'azione penale a livello di Stato membro. Le norme sulla protezione dei dati dell'EPPO sono, pertanto, quasi identiche a quelle

della direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali. Ai sensi della proposta di istituzione dell’EPPO, il trattamento dei dati personali deve rispettare i principi di liceità e correttezza, limitazione della finalità, minimizzazione dei dati, esattezza, integrità e riservatezza. Per quanto possibile, l’EPPO deve operare una chiara distinzione tra i dati personali dei diversi tipi di interessati, come le persone condannate o semplicemente sospettate di aver commesso un reato, vittime e testimoni. Deve inoltre cercare di verificare la qualità dei dati personali trattati e, per quanto possibile, distinguere i dati personali basati su fatti dai dati basati su valutazioni personali.

La proposta contiene disposizioni sui diritti degli interessati, segnata- mente i diritti di informazione, di accesso ai propri dati personali, di rettifica,

cancellazione e limitazione del trattamento, e prevede che tali diritti possano essere esercitati anche indirettamente, tramite il GEPD. Essa incorpora, inol- tre, i principi di sicurezza del trattamento e di responsabilizzazione, imponendo all'EPPO di attuare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato ai rischi che il trattamento comporta, di tenere reg- istri di tutte le attività di trattamento dei dati e di effettuare una valutazione d'impatto sulla protezione dei dati prima del trattamento, qualora un tipo di trat- tamento (ad esempio, un trattamento che prevede l'uso di nuove tecnologie) sia suscettibile di presentare un rischio elevato per i diritti delle persone. Infine, la proposta prevede la designazione, da parte del collegio, di un responsabile della protezione dei dati, che deve essere adeguatamente coinvolto in tutte le ques- tioni riguardanti la protezione dei dati personali e garantire il rispetto da parte dell'EPPO della legislazione applicabile in materia di protezione dei dati.

8.3.2. Protezione dei dati nei sistemi d'informazione comune a livello dell'UE

Oltre allo scambio di dati fra Stati membri e alla creazione di autorità dell'Unione specializ zate nella lotta contro la criminalità transfrontaliera, come Europol, Eurojust ed EPPO, a livello dell'UE, sono stati istituiti diversi sis- temi d'informazione comune per permettere e facilitare

la cooperazione e lo scambio di dati fra le autorità nazionali e dell'UE competenti per fini specifici in materia di protezione delle frontiere, immigrazione, asilo e dogane. Poi- ché lo spazio Schengen è originariamente stato creato mediante un accordo internazionale operante in modo indipendente dal diritto dell'UE, il Sistema d'informazione Schengen (SIS) è stato sviluppato a partire da accordi multilat- erali, e successivamente integrato nel diritto dell'UE. Il sistema di informazione visti (VIS), Eurodac, Eurosur e il sistema informativo doganale (SID) sono stati creati come strumenti disciplinati dal diritto dell'UE.

Il controllo di questi sistemi è condiviso tra le autorità nazionali di controllo e il GEPD. Per garantire un livello di protezione elevato, tali autorità collaborano nell'ambito dei gruppi di coordinamento della supervisione, che fanno riferi- mento ai seguenti sistemi informativi su larga scala: 1) Eurodac; 2) sistema di informazione visti; 3) sistema d'informazione Schengen; 4) sistema informativo doganale e 5) sistema d'informazione del mercato interno[843]. I gruppi di coordi-

namento della supervisione si riuniscono solitamente due volte all’anno sotto l’autorità di un presidente eletto e adottano linee guida, discutono casi trans- frontalieri o adottano regimi comuni per le ispezioni.

L’Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu- LISA)[844], istituita nel 2012, è responsabile della gestione operativa del sis- tema d’Informazione Schengen di seconda generazione (SIS II), del sistema di informazione visti (VIS) e di Eurodac. Il compito principale di eu-LISA è quello di garantire un esercizio efficace, sicuro e continuo dei sistemi IT. L’Agenzia è anche responsabile dell’adozione di misure necessarie a garantire la sicurezza dei sistemi e dei dati.

Il sistema d’informazione Schengen

Nel 1985 diversi Stati membri dell’allora Comunità europea hanno stipulato l’accordo fra gli Stati dell’Unione economica del Benelux, la Germania e la Francia per l’eliminazione graduale dei controlli alle frontiere comuni (accordo Schengen), con l’intento di creare uno spazio per la libera circolazione delle persone, esente da controlli di frontiera nel territorio Schengen[845]. Per controbi- lanciare la minaccia alla sicurezza pubblica che potrebbe derivare dall’apertura delle frontiere, sono stati istituiti controlli di frontiera rafforzati alle frontiere esterne dello spazio Schengen ed è stata

avviata una stretta cooperazione tra le autorità nazionali di polizia e giudiziarie.

A seguito dell’adesione di altri Stati all’accordo Schengen, il relativo sistema è stato integrato in via definitiva nel quadro giuridico dell’UE con il trat- tato di Amsterdam[846]. L’attuazione di questa decisione è avvenuta nel 1999. La versione più recente del sistema d’informazione Schengen, il cosiddetto SIS II, è divenuta operativa il 9 aprile 2013. Attualmente riguarda la maggior

parte degli Stati membri dell’UE[847] oltre a Islanda, Liechtenstein, Norvegia e
Svizzera[848]. Anche Europol e l’Eurojust hanno accesso a SIS II.

SIS II è costituito da un sistema centrale (SIS-C), da un sistema nazionale (SIS-N) in ciascuno Stato membro e da un’infrastruttura di comunicazione fra il sis- tema centrale e i sistemi nazionali. Il SIS-C contiene alcuni dati inseriti dagli Stati membri su persone e oggetti ed è usato dalle autorità nazionali preposte ai con- trolli di frontiera, dalle autorità di polizia, dalle autorità doganali, dalle autorità competenti al rilascio dei visti e dalle autorità giudiziarie nello spazio Schengen. Ogni Stato membro gestisce una copia nazionale del SIS-C, nota come sistema d’informazione Schengen nazionale (SIS-N), costantemente aggiornata, aggior- nando così anche il SIS-C. Nel SIS esistono diversi tipi di segnalazioni:

- la persona non ha il diritto d’ingresso o di soggiorno nel territorio Schen- gen; o

- la persona o l’oggetto sono ricercati da autorità giudiziarie o da autorità preposte all’applicazione della legge (ad esempio, mandati d’arresto euro- pei, richieste di sorveglianza discreta); o

- la persona è stata segnalata come scomparsa; o

- beni quali banconote, automobili, veicoli commerciali, armi e documenti d'identità sono stati denunciati come beni rubati o smarriti.

In caso di segnalazione, le attività di follow-up devono essere avviate attra- verso gli uffici SIRENE. Il SIS II dispone di nuove funzionalità, fra cui la pos- sibilità di inserire dati biometrici, quali impronte digitali e fotografie; nuove categorie di segnalazioni, quali imbarcazioni, aeromobili, container o mezzi di pagamento rubati; migliori segnalazioni su persone e oggetti e copie dei man- dati d'arresto europei (MAE) relativi a persone ricercate a fini di arresto, con- segna o estradizione.

Il SIS II si basa su due atti complementari: la decisione SIS II[849] e il regolamento SIS II[850]. Per l'adozione della decisione e del regolamento, il legislatore dell'UE ha utilizzato basi giuridiche diverse. La decisione disciplina l'uso del SIS II per finalità nell'ambito della cooperazione giudiziaria e di polizia in materia penale (ex terzo pilastro dell'UE). Il regolamento si applica alle procedure di segnalazione relative a visti, asilo, immigrazione e altre politiche relative alla libera circolazione delle per- sone (ex primo pilastro). Le procedure di segnalazione per ciascun pilastro dove- vano essere regolate da atti separati, dal momento che i due atti giuridici erano stati adottati prima del trattato di Lisbona e della soppressione della struttura a pilastri.

Entrambi gli atti giuridici contengono norme in materia di protezione dei dati. La decisione SIS II vieta il trattamento dei dati sensibili[851]. Il trattamento dei dati personali rientra nell'ambito di applicazione della Convenzione n. 108 modern- izzata[852]. Inoltre, le persone hanno il diritto di accesso ai dati personali che le riguardano inseriti nel SIS II[853].

Il regolamento SIS II disciplina le condizioni e le procedure applicabili all'inserimento e al trattamento delle segnalazioni relative a rifiuti d'ingresso o di soggiorno a cittadini di paesi terzi. Esso prevede inoltre disposizioni rel- ative allo scambio di informazioni supplementari e

complementari ai fini dell'ingresso o del soggiorno in uno Stato membro[854]. Il regolamento contiene altresì disposizioni in materia di protezione dei dati. È vietato il trattamento delle categorie di dati sensibili di cui all'articolo 9, paragrafo 1, del regolamento generale sulla protezione dei dati[855]. Il regolamento SIS II contiene anche taluni diritti a favore dell'interessato, e precisamente:

- il diritto di accesso ai dati personali che lo riguardano[856];

- il diritto di far rettificare dati contenenti errori di fatto[857];

• il diritto di far cancellare dati inseriti illecitamente[858]; e

• il diritto di essere informato in merito a segnalazioni effettuate nei suoi confronti. Le informazioni sono fornite per iscritto insieme a una copia della decisione nazionale che ha dato origine alla segnalazione[859].

Le informazioni non sono fornite qualora 1) i dati personali non siano stati rac- colti presso l'interessato e a condizione che la fornitura di tale informazione sia impossibile o richieda sforzi sproporzionati, 2) l'interessato sia già in possesso delle informazioni o 3) la legislazione nazionale permetta una limitazione, fra l'altro, per salvaguardare la sicurezza nazionale o prevenire reati[860].

Sia per la decisione SIS II sia per il regolamento SIS II, i diritti di accesso delle per- sone con riferimento al SIS II possono essere esercitati in ogni Stato membro e saranno trattati nel rispetto della legislazione nazionale di tale Stato membro[861].

Esempio: nella causa *Dalea c. Francia*[862], al ricorrente era stato negato un visto per entrare in Francia poiché le autorità francesi avevano segnalato al sistema d'informazione Schengen la necessità di negargli

l'ingresso. Il ricorrente aveva chiesto, senza esito positivo, l'accesso e la rettifica o la cancellazione dei dati alla commissione francese per la protezione dei dati e, in ultima istanza, al Consiglio di Stato. La Corte EDU ha statuito che l'inserimento del ricorrente nel sistema d'informazione Schengen era stato conforme alla legge e aveva perseguito lo scopo legittimo di tutelare la sicurezza nazionale. Poiché il ricorrente non aveva dimostrato quale danno avesse effettivamente subito a causa del negato ingresso nello spazio Schengen, e poiché erano state attuate misure sufficienti per tutelarlo da decisioni arbitrarie, l'ingerenza nel suo diritto al rispetto della vita privata era stata proporzionata. Pertanto, il ricorso del ricorrente ai sensi dell'articolo 8 è stato dichiarato irricevibile.

L'autorità nazionale di controllo competente in ciascuno Stato membro cont- rolla il SIS-N interno. L'autorità nazionale di controllo deve provvedere affin- ché venga effettuata una verifica delle operazioni di trattamento dei dati nel

SIS-N interno almeno ogni quattro anni[863]. Le autorità nazionali di controllo e il GEPD cooperano e garantiscono il controllo coordinato del SIS N, mentre il GEPD è responsabile della supervisione del SIS-C. A fini di trasparenza, ogni due anni deve essere trasmessa al Parlamento europeo, al Consiglio e a eu- LISA una relazione congiunta sulle attività svolte. Il gruppo di coordinamento della supervisione del SIS II è stato istituito per garantire il coordinamento della supervisione del SIS e si riunisce due volte all'anno. Tale gruppo è composto dal GEPD e dai rappresentanti delle autorità di controllo degli Stati membri che hanno attuato il SIS II, nonché Islanda, Liechtenstein, Norvegia e Svizzera, dal momento che il SIS si applica anche a tali paesi, in quanto membri di Schen- gen[864]. Cipro, Croazia e Irlanda non hanno ancora aderito al SIS II e, pertanto, partecipano al gruppo di coordinamento della supervisione solamente in qual- ità di osservatori. Nell'ambito del gruppo di coordinamento della supervisione, il GEPD e le autorità nazionali di controllo cooperano attivamente scambiandosi informazioni, assistendosi vicendevolmente nello svolgimento di revisioni e ispezioni, elaborando proposte armonizzate per soluzioni congiunte di eventu- ali problemi e promuovendo la sensibilizzazione in materia di diritti di protezi- one dei dati[865]. Anche il gruppo di coordinamento della supervisione del SIS II adotta linee guida per assistere gli interessati. Un esempio

è costituito dalla guida all’esercizio dei diritti di accesso destinata agli interessati[866].

Prospettiva

Nel 2016, la Commissione europea ha effettuato una valutazione del SIS[867], mostrando che meccanismi nazionali sono stati messi in atto per consentire agli interessati di accedere, rettificare e cancellare i loro dati personali nel SIS II o ottenere un risarcimento in relazione a dati inesatti. Per migliorare l’efficienza e l’efficacia del SIS II, la Commissione europea ha presentato tre proposte di regolamento:

- un regolamento sull’istituzione, l’esercizio e l’uso del SIS nel settore delle verifiche di frontiera, che abrogherà il regolamento SIS II;

- un regolamento sull’istituzione, l’esercizio e l’uso del SIS nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che abrogherà, fra l’altro, la decisione SIS II; e

- un regolamento relativo all’uso del SIS per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare.

È importante sottolineare che le proposte consentono il trattamento di altre categorie di dati biometrici, oltre alle fotografie e alle impronte digitali, che fanno già parte dell’attuale sistema SIS II. Nella banca dati del SIS saranno con- servate anche immagini facciali, impronte palmari e i profili DNA. Inoltre, men- tre il regolamento SIS II e la decisione SIS II prevedevano la possibilità di effet- tuare un’interrogazione con le impronte digitali per identificare una persona, le proposte rendono obbligatoria tale consultazione qualora l’identità della per- sona non possa essere accertata in altro modo. Immagini facciali, fotografie e immagini palmari saranno utilizzate per consultare il sistema e identificare le persone non appena ciò diviene tecnicamente possibile. Le nuove norme sugli attributi biometrici presentano rischi particolari per i diritti delle persone. Nel suo parere sulle proposte della Commissione[868], il GEPD ha osservato che i dati biometrici sono altamente sensibili e la loro introduzione in una tale banca dati su larga scala dovrebbe basarsi su una valutazione della necessità

di inser- irli nel SIS fondata sulle prove. In altre parole, la necessità del trattamento dei nuovi attributi dovrebbe essere dimostrata. Il GEPD ha inoltre considerato la necessità di chiarire ulteriormente il tipo di informazioni che possono essere inserite nel profilo DNA. Dal momento che il profilo del DNA può includere informazioni sensibili (l'esempio più significativo è costituito dalle informazi- oni sulla salute), i profili DNA archiviati nel SIS dovrebbero contenere «unica- mente le informazioni minime strettamente necessari per l'identificazione delle persone scomparse ed escludere esplicitamente le informazioni relative alla salute, alla razza e ad altre informazioni sensibili»[869]. Le proposte, tutta- via, prevedono salvaguardie aggiuntive per limitare la raccolta e il successivo trattamento dei dati a quanto strettamente necessario e indispensabile dal punto di vista operativo, e l'accesso ai dati personali è limitato alle persone

che hanno l'esigenza di trattarli a fini operativi[870]. Le proposte incaricano altresì eu-LISA di fornire agli Stati membri relazioni sulla qualità dei dati a scadenze regolari, per permettere loro di riesaminare periodicamente le segnalazioni al fine di garantire la qualità dei dati[871].

Il sistema di informazione visti

Il sistema di informazione visti (VIS), anch'esso gestito da eu-LISA, è stato svi- luppato per sostenere l'attuazione di una politica comune dell'UE in materia di visti[872]. Il sistema VIS consente agli Stati Schengen di scambiarsi informazioni sui visti mediante un sistema totalmente centralizzato che collega i consolati e le ambasciate degli Stati Schengen ubicati in paesi extra-UE con i punti di attraver- samento delle frontiere esterne di tutti gli Stati Schengen. Il sistema VIS tratta dati concernenti le domande di visti relativi a soggiorni di breve durata per l'ingresso o il transito attraverso lo spazio Schengen. Esso consente alle autorità di frontiera di verificare, con l'aiuto di attributi biometrici, segnatamente le impronte digitali, se la persona che presenta un visto sia o meno il legittimo titolare e di identificare le persone prive di documenti o in possesso di documenti falsi.

Il regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio concer- nente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati

membri sui visti per soggiorni di breve durata (regolamento VIS) disciplina le condizioni e le procedure per il trasferimento dei dati personali riguardanti domande di visti per soggiorni di breve durata. Esso controlla le decisioni adottate in ordine alle domande, comprese le decisioni in materia di annullamento, revoca o pro- roga del visto[873]. Il regolamento VIS riguarda principalmente i dati relativi al richiedente, i suoi visti, fotografie, impronte digitali, collegamenti con domande

precedenti, i fascicoli relativi alla domanda delle persone che lo accompagnano o dati riguardanti le persone che hanno formulato un invito[874].
L'accesso al VIS per inserire, modificare o cancellare dati è limitato esclusivamente alle autorità competenti per il rilascio dei visti, mentre l'accesso a fini di consultazione dei dati è previsto per le autorità competenti in materia di rilascio dei visti e per le autorità competenti in materia di controlli ai punti di attraversamento delle frontiere esterne, di controlli sull'immigrazione e di domande di asilo.

A determinate condizioni, le autorità nazionali competenti per la pubblica sicurezza ed Europol possono chiedere l'accesso ai dati registrati nel VIS ai fini della prevenzione, dell'individuazione o dell'investigazione di reati di terrorismo e altri reati gravi[875]. Poiché il VIS è stato concepito come uno strumento a sostegno dell'attuazione della politica comune in materia di visti, il principio della limitazi- one delle finalità che, come spiegato nel capitolo 3.2, richiede che i dati personali siano trattati soltanto con riferimento a persone specifiche, esplicite e legittime e devono essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali vengono trattati, sarebbe violato se il VIS diventasse uno strumento di applicazi- one della legge. Per questa ragione, alle autorità preposte all'applicazione della legge e a Europol è negato l'accesso sistematico alla banca dati VIS. L'accesso può essere consentito solo in casi specifici e in presenza di garanzie rigorose. Le

condizioni e le garanzie per l'accesso e la consultazione del VIS da parte di tali autorità sono disciplinate nella decisione 2008/633/GAI del Consiglio[876].

Inoltre, il regolamento VIS prevede diritti per gli interessati, e precisamente:

- il diritto di essere informati dallo Stato membro competente circa l'identità e i dati di contatto del titolare del trattamento dei dati personali in tale Stato membro, le finalità per le quali i dati saranno trattati nell'ambito del VIS, le categorie delle persone alle quali i dati possono essere trasmessi (destina- tari) e il periodo di conservazione degli stessi. Inoltre, i richiedenti il visto devono essere informati del fatto che l'acquisizione dei loro dati personali ai sensi del VIS è obbligatoria ai fini dell'esame della domanda, mentre gli Stati

membri devono anche informarli in merito all'esistenza del diritto di accesso ai dati che li riguardano, di chiedere che siano rettificati o cancellati, e in merito alle procedure che permettono loro di esercitare tali diritti[877].

- Il diritto di accesso delle persone ai dati personali registrati nel VIS che le riguardano[878].

- Il diritto di rettifica di dati inesatti[879].

- Il diritto alla cancellazione di dati registrati illegittimamente[880].

Per garantire il controllo del VIS è stato istituito un gruppo di coordinamento della supervisione. Esso è composto da rappresentanti del GEPD e autorità nazionali di controllo, che si riuniscono due volte all'anno. Questo gruppo è composto da rappresentanti dei 28 Stati membri dell'UE nonché Islanda, Liech- tenstein, Norvegia e Svizzera[881].

Eurodac

Il termine Eurodac si riferisce al sistema europeo di dattiloscopia. Si tratta di un sistema centralizzato che contiene i dati relativi alle impronte digitali di cit- tadini di paesi terzi e apolidi che presentano domanda di asilo in uno degli Stati membri dell'UE[882]. Il sistema è operativo dal gennaio 2003,

con l’adozione del regolamento del Consiglio n. 2725/2000; una rifusione è entrata in vigore nel

2015. Il suo scopo è principalmente di concorrere alla determinazione dello Stato membro competente per l'esame di una specifica domanda d'asilo ai sensi del regolamento (CE) n. 604/2013. Tale regolamento stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide (regolamento Dublino III)[883]. I dati personali nell'Eurodac hanno lo scopo principale di facilitare l'applicazione del regolamento Dublino III[884].

Le autorità preposte all'applicazione della legge ed Europol possono confron- tare le impronte digitali collegate a un'indagine penale con le impronte digi- tali contenute nell'Eurodac, ma solo al fine di prevenire, accertare o investigare reati di terrorismo o altri reati gravi. Poiché Eurodac è stato concepito come strumento di supporto all'attuazione della politica di asilo dell'UE e non come strumento di applicazione della legge, le autorità di contrasto hanno accesso alla banca dati unicamente in casi specifici, in circostanze ben definite e sotto rigide condizioni[885]. Per l'ulteriore utilizzo dei dati a fini di contrasto, si applica la direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, mentre i dati utilizzati con lo scopo principale di agevolare l'applicazione del regolamento Dublino III sono tutelati dal regolamento generale sulla pro- tezione dei dati. L'ulteriore trasferimento di dati

personali ottenuti da uno Stato membro o da Europol ai sensi del regolamento Eurodac rifuso verso paesi terzi, organizzazioni internazionali o soggetti di diritto privato stabiliti all'interno o all'esterno dell'UE è vietato[886].

L'Eurodac comprende un'unità centrale, gestita da eu-LISA, che conserva e con- fronta le impronte digitali nonché un sistema per la trasmissione elettronica dei dati fra gli Stati membri e la banca dati centrale. Gli Stati membri rilevano e trasmettono le impronte digitali di ogni persona di età maggiore di 14 anni che richieda asilo nel loro territorio e di ogni cittadino extra-UE o apolide di età maggiore di 14 anni che sia fermato per attraversamento non autorizzato della loro frontiera esterna. Gli Stati membri possono anche rilevare e trasmettere le

impronte digitali di cittadini extra-UE o di apolidi soggiornanti nel loro territorio senza permesso.

Anche se qualsiasi Stato membro può consultare Eurodac e chiedere il con- fronto con i dati relativi alle impronte digitali, soltanto lo Stato membro che ha rilevato le impronte digitali e le ha trasmesse al sistema centrale ha il diritto di modificare i dati rettificandoli, integrandoli o cancellandoli[887]. Eu-LISA conserva le registrazioni di tutti i trattamenti dei dati avvenuti nel sistema centrale per controllare la protezione dei dati e garantirne la sicurezza[888]. Le autorità nazi- onali di controllo prestano assistenza e consulenza agli interessati nell'esercizio dei loro diritti[889] Il rilevamento e la trasmissione delle impronte digitali è sog- getto a controllo giurisdizionale da parte delle autorità nazionali[890]. Il regola- mento sulla protezione dei dati da parte delle istituzioni dell'UE[891] e la vigilanza del GEPD si applicano alle attività di trattamento del sistema centrale, che è gestito da eu-LISA relativamente a Eurodac[892]. Le persone che subiscono un danno in conseguenza di un trattamento illecito di dati o di qualsiasi altro atto incompatibile con il regolamento Eurodac hanno diritto di ottenere un risar- cimento dallo Stato membro responsabile del pregiudizio[893]. Va sottolineato, tuttavia, che i richiedenti asilo sono un gruppo particolarmente vulnerabile di persone, che spesso hanno intrapreso viaggi lunghi e rischiosi. A

causa della loro vulnerabilità e della situazione precaria in cui spesso si trovano mentre è in corso l'esame della loro domanda di asilo, in pratica l'esercizio dei loro diritti, compreso il diritto al risarcimento, può rivelarsi difficile.

Per utilizzare Eurodac a fini di contrasto, gli Stati membri devono designare le autorità che avranno il diritto di richiedere l'accesso nonché le autorità che verificheranno che le richieste di confronto siano legittime[894]. L'accesso delle autorità nazionali e di Europol ai dati dattiloscopici di Eurodac è soggetto a condizioni molto rigorose. L'autorità richiedente deve presentare una richiesta

elettronica motivata solo dopo aver confrontato i dati con quelli di altri sistemi di informazione disponibili, come le banche dati nazionali di dati dattiloscopici e il VIS. Deve esistere un interesse prevalente di sicurezza pubblica che rende il confronto proporzionato. Il confronto deve essere realmente necessario, deve riguardare un caso specifico e devono sussistere fondati motivi per ritenere che il confronto contribuirà in modo sostanziale alla prevenzione, all'accertamento o all'investigazione di qualsiasi dei reati in questione, in particolare quando sussiste il sospetto fondato che l'autore presunto o effettivo oppure la vittima di un reato di terrorismo o di un altro reato grave rientri in una delle catego- rie per le quali è previsto il rilevamento delle impronte digitali nell'ambito del sistema Eurodac. Il confronto deve essere effettuato esclusivamente con i dati relativi alle impronte digitali. Europol deve inoltre ottenere l'autorizzazione dello Stato membro che ha raccolto i dati relativi alle impronte digitali.

I dati personali archiviati in Eurodac e relativi ai richiedenti asilo sono con- servati per 10 anni dalla data di rilevamento delle impronte digitali, a meno che l'interessato non ottenga la cittadinanza di uno Stato membro dell'UE. In tal caso, i dati devono essere cancellati immediatamente. I dati relativi agli stranieri fermati per attraversamento non autorizzato della frontiera esterna sono conservati per 18 mesi e devono essere cancellati

immediatamente se l’interessato ottiene un permesso di soggiorno, lascia il territorio dell’Unione o acquisisce la cittadinanza di uno Stato membro. I dati delle persone che hanno ottenuto asilo restano disponibili per il confronto a fini di prevenzione, accer- tamento o investigazione di reati di terrorismo o altri reati gravi per un periodo di tre anni.

Oltre a tutti gli Stati membri dell’UE, anche Islanda, Norvegia, Liechtenstein e
Svizzera si avvalgono dell’Eurodac sulla base di accordi internazionali.

Il gruppo di coordinamento della supervisione è stato istituito per assicurare il controllo dell’Eurodac. Esso è composto da rappresentanti del GEPD e autorità nazionali di con- trollo, che si riuniscono due volte all’anno. Questo gruppo è composto da rappresent- anti dei 28 Stati membri dell’UE nonché Islanda, Liechtenstein, Norvegia e Svizzera[895].

Prospettiva

Nel maggio 2016, la Commissione ha presentato una proposta per un nuovo regola- mento Eurodac rifuso, nell’ambito di una riforma volta a migliorare il funzionamento

del sistema europeo comune di asilo (CEAS)[896]. La rifusione proposta è importante in quanto amplierà in modo significativo il campo di applicazione della banca dati Eurodac originale. Eurodac è stato inizialmente creato per sostenere l'attuazione del CEAS, fornendo prove dattiloscopiche per consentire di determinare lo Stato membro competente per l'esame di una domanda d'asilo presentata nell'Unione. La rifusione proposta estenderà l'ambito della banca dati per facilitare il rimpatrio dei migranti in situazione irregolare[897]. Le autorità nazionali potranno consultare la banca dati al fine di identificare i cittadini di paesi terzi il cui soggiorno nell'UE è irregolare o che sono entrati nell'UE in maniera irregolare, al fine di ottenere elementi di prova utili agli Stati membri per poter rimpatriare tali persone. Inoltre, mentre il regime giuridico attual- mente in vigore prevede solo il rilevamento e la conservazione delle impronte digi- tali, la proposta introduce il rilevamento di immagini del volto delle persone[898], che è un tipo diverso di dato biometrico. La proposta abbasserebbe altresì a 6 anni[899] l'età minima per il rilevamento dei dati biometrici dei minori, anziché 14 anni, che è l'età minima prevista dal regolamento del 2013. L'estensione dell'ambito di applicazione della proposta significa che essa costituirà un'ingerenza nei diritti alla vita privata e alla protezione dei dati di un maggior numero di persone che potrebbero essere inserite nella banca dati. Per controbilanciare tale ingerenza, la proposta e gli emendamenti proposti dalla

commissione LIBE del Parlamento europeo[900]
intendono rafforzare i

requisiti in materia di protezione dei dati. Al momento della stesura di questo manuale, le discussioni sulla proposta nell'ambito del Parlamento e del Consiglio erano in corso.

Eurosur

Il sistema europeo di sorveglianza delle frontiere (Eurosur)[901] è volto a miglio- rare il controllo delle frontiere esterne Schengen individuando, prevenendo e combattendo l'immigrazione irregolare e la criminalità transfrontaliera. Il sis- tema serve a rafforzare lo scambio di informazioni e la cooperazione opera- tiva fra i centri di coordinamento nazionale e Frontex, l'agenzia dell'UE per lo sviluppo e l'applicazione del nuovo concetto di gestione integrata delle fron- tiere[902]. Gli obiettivi generali di Eurosur sono:

• ridurre il numero di migranti irregolari che entrano nell'UE in modo clandestino;

• ridurre il numero di decessi di migranti irregolari salvando più vite in mare;

• aumentare la sicurezza interna dell'UE nel suo insieme contribuendo a pre- venire la criminalità transfrontaliera[903].

Eurosur è divenuto operativo il 2 dicembre 2013 in tutti gli Stati membri con frontiere esterne e il 1°

dicembre 2014 negli altri Stati. Il regolamento si applica alla sorveglianza delle frontiere esterne terrestri, marittime e aeree degli Stati membri. Eurosur scambia e tratta dati personali in misura molto limitata, dal momento che gli Stati membri e Frontex sono autorizzati a scambiare solo i numeri di identificazione delle navi. Eurosur scambia informazioni opera- tive, come l'ubicazione di pattuglie e incidenti e, come regola generale, le

informazioni scambiate non possono includere dati personali[904]. In casi eccezi- onali in cui i dati personali vengono scambiati nell'ambito della struttura di Eurosur, il regolamento prevede che il quadro giuridico generale dell'UE sulla protezione dei dati sia pienamente applicabile[905].

Eurosur garantisce pertanto il diritto alla protezione dei dati, in particolare, affer- mando che gli scambi di dati personali devono rispettare i criteri e le garanzie sanciti dalla direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali e dal regolamento generale sulla protezione dei dati[906].

Il sistema informativo doganale

Un altro importante sistema d'informazione comune attuato a livello di UE è il sistema informativo doganale (SID)[907]. Nel quadro dell'istituzione di un mer- cato interno, sono stati aboliti tutti i controlli e le formalità relativi alle merci che circolano nel territorio dell'UE, con conseguente aumento del rischio di frode. Il maggiore rischio di frode che ne è derivato è stato controbilanciato da una più intensa cooperazione fra le amministrazioni doganali degli Stati mem- bri. Lo scopo del SID è quello di sostenere gli Stati membri nella prevenzione, nell'indagine e nel perseguimento di gravi violazioni delle leggi nazionali e dell'UE in materia doganale e agricola. Il

SID è costituito da due atti giuridici, adottati su basi giuridiche diverse: il regolamento (CE) n. 515/97 del Consiglio riguarda la cooperazione tra diverse autorità amministrative nazionali per lot- tare contro le frodi nell'ambito dell'unione doganale e della politica agricola comune, mentre la decisione 2009/917/GAI del Consiglio ha lo scopo di facili- tare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali. Questo significa che il SID non riguarda solo l'applicazione della legge.

Le informazioni contenute nel SID comprendono dati personali relativi a merci, mezzi di trasporto, imprese, persone, articoli e denaro bloccati, sequestrati o confiscati. Le categorie di dati che possono essere trattati sono definite chi- aramente e comprendono nomi, cittadinanza, sesso, luogo e data di nascita delle persone interessate, ragione dell'inserimento dei loro dati nel sistema e numero d'immatricolazione del mezzo di trasporto[908]. Queste informazioni pos- sono essere utilizzate unicamente a fini di osservazione e di rendiconto, di con- trolli specifici e di analisi strategica o operativa concernenti persone sospettate di violazione delle disposizioni doganali.

L'accesso al SID è concesso alle autorità nazionali doganali, fiscali, agricole, sanitarie pubbliche e di polizia nonché a Europol e all'Eurojust.

Il trattamento di dati personali dev'essere effettuato nel rispetto delle norme specifiche di cui al regolamento n. 515/97 e alla decisione 2009/917/GAI del Consiglio nonché delle disposizioni del regolamento generale sulla protezi- one dei dati, del regolamento sulla protezione dei dati da parte delle istituzi- oni dell'UE, della Convenzione n. 108 modernizzata e della raccomandazione relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza. Il GEPD è responsabile di controllare la conformità del SID con il regolamento

(CE) n. 45/2001. Esso convoca almeno una volta all’anno una riunione con tutte le autorità nazionali garanti della protezione dei dati compe- tenti per le questioni di controllo relative al SID.

Interoperabilità tra i sistemi informatici dell’UE

La gestione delle migrazioni, la gestione integrata delle frontiere esterne dell’UE e la lotta al terrorismo e alla criminalità transfrontaliera pongono sfide importanti e sono diventate sempre più complesse in un mondo globalizzato. Negli ultimi anni l’UE lavora a un nuovo approccio globale per salvaguardare e mantenere la sicurezza, senza compromettere i sui valori e le sue libertà fondamentali. A tal fine, uno scambio di informazioni efficace tra le autorità di contrasto nazionali e tra gli Stati membri e le pertinenti agenzie dell’UE, è

fondamentale[909]. Gli attuali sistemi di informazione dell'UE per la gestione delle frontiere e la sicurezza interna hanno i loro rispettivi obiettivi, quadri istituzi- onali, interessati e utenti. L'UE si adopera per ovviare alle carenze nelle fun- zionalità della gestione frammentaria dei dati dell'UE tra i diversi sistemi di informazione, quali SIS II, VIS ed Eurodac, esplorando le possibilità di interop- erabilità[910]. L'obiettivo principale è garantire che le autorità di polizia, doganali e giudiziarie competenti dispongano sistematicamente delle informazioni nec- essarie per svolgere le loro funzioni, mantenendo al contempo un equilibrio per quanto riguarda i diritti alla vita privata, alla protezione dei dati e ad altri diritti fondamentali.

L'interoperabilità è «la capacità di sistemi di informazione di scambiare dati e di consentire la condivisione delle informazioni»[911]. Tale scambio non deve com- promettere le norme necessariamente rigorose sull'accesso e sull'utilizzo gar- antite dal regolamento generale sulla protezione dei dati, dalla direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, dalla Carta dei diritti fondamentali dell'Unione europea e da tutte le altre norme per- tinenti. Qualsiasi soluzione integrata della gestione dei dati non deve compro- mettere i principi di limitazione delle finalità, protezione dei dati fin dalla pro- gettazione o protezione dei dati di default[912].

Oltre a migliorare le funzionalità dei tre principali sistemi di informazione – SIS II, VIS ed Eurodac – la Commissione ha proposto l'istituzione di un quarto sistema centralizzato di gestione delle frontiere che riguarda i cittadini di paesi terzi: il sistema di ingressi/uscite (EES)[913], che dovrebbe essere completato entro il 2020[914]. La Commissione ha inoltre presentato una proposta di istituzi- one di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)[915], un sistema che raccoglierà informazioni sulle persone che viaggiano senza obbligo di visto nell'UE, per consentire controlli preventivi sulla migrazione irregolare e di sicurezza.

In diverse circostanze, a livello europeo, sono stati adottati strumenti giuridici particolari per applicare con maggior precisione le norme generali della Convenzione n. 108 modernizzata o del regolamento generale sulla protezione dei dati a situazioni specifiche.

9.1. Comunicazioni elettroniche

- La raccomandazione del CdE del 1995 contiene norme specifiche sulla protezione dei dati nel settore delle telecomunicazioni, con particolare riguardo ai servizi telefonici.

- Il trattamento dei dati personali relativi alla prestazione di servizi di comunicazi- one a livello di UE è regolamentato nella direttiva relativa alla vita privata e alle comunicazioni elettroniche.

- La riser vatezza delle comunicazioni elettroniche non si limita al contenuto di una comunicazione, ma si estende anche ai metadati, quali le informazioni su chi ha comunicato con chi, quando e per quanto tempo, nonché ai dati relativi all'ubicazione, come il luogo dal quale sono stati comunicati i dati.

Le reti di comunicazione hanno un maggiore potenziale di ingerenza ingiusti- ficata nella sfera personale degli utenti, poiché comportano efficaci possibilità tecniche di ascoltare e controllare le comunicazioni effettuate attraverso tali reti. Di conseguenza, si è ritenuto necessario adottare specifiche norme sulla protezione dei dati per fare fronte ai rischi specifici corsi dagli utenti dei servizi di comunicazione.

Nel 1995 il CdE ha emanato una raccomandazione relativa alla protezione dei dati nel settore delle telecomunicazioni, con particolare riguardo ai servizi tel- efonici[916]. Secondo questa raccomandazione, i dati personali nel contesto delle telecomunicazioni dovrebbero essere raccolti e trattati unicamente ai fini della connessione di un utente alla rete e della fornitura di un determinato servizio di telecomunicazione nonché per la fatturazione e la verifica del pagamento, per assicurare un'installazione tecnica ottimale e lo sviluppo della rete e del servizio.

Particolare attenzione è stata dedicata anche all'uso delle reti di comunicazi- one per l'invio di messaggi di marketing diretto. In generale, tali messaggi non possono essere inviati nei confronti di un abbonato che abbia espresso il desi- derio di non riceverli. I dispositivi di chiamata automatica per la trasmissione di messaggi preregistrati di natura pubblicitaria possono essere usati soltanto se gli

abbonati hanno accordato il proprio consenso esplicito. La legislazione nazi- onale deve prevedere norme specifiche in questo settore.

Nell'ambito del quadro giuridico dell'UE, dopo un primo tentativo nel 1997, nel 2002 è stata adottata la direttiva relativa alla vita privata e alle comunicazioni elettroniche, modificata poi nel 2009 al fine di integrare e adeguare le disposizioni della precedente direttiva sulla tutela dei dati nel settore delle telecomunicazioni[917].

L'applicazione della direttiva relativa alla vita privata e alle comunicazioni elet troniche è limitata ai ser vizi di comunicazione nelle reti elet troniche pubbliche.

La direttiva relativa alla vita privata e alle comunicazioni elettroniche distingue tre categorie principali di dati generati nel corso di una comunicazione:

- i dati che costituiscono il contenuto dei messaggi inviati durante la comuni- cazione: si tratta di dati strettamente riservati;

- i dati necessari per stabilire e mantenere la comunicazione: i cosiddetti metadati, ai quali la direttiva fa riferimento come «dati relativi al traffico», quali informazioni sugli interlocutori, sul momento e sulla durata della comunicazione;

- fra i metadati figurano dati specificamente connessi all'ubicazione del dis- positivo di comunicazione, i cosiddetti dati relativi all'ubicazione; tali dati riguardano al contempo l'ubicazione degli utenti dei dispositivi di comuni- cazione, in particolare per quanto concerne gli utenti di dispositivi di comu- nicazione mobile.

I dati relativi al traf fico possono essere usati dal fornitore di ser vizi solo ai fini della fat turazione e della fornitura tecnica del ser vizio. Con il con-

senso dell’interessato, tuttavia, questi dati possono essere divulgati ad altri titolari del trattamento che offrono ser vizi a valore aggiunto, quali la for- nitura di informazioni, in base all’ubicazione dell’utente, riguardanti la stazi- one di metropolitana o la farmacia più vicine o le previsioni del tempo per quell’ubicazione.

Altre forme di accesso ai dati relativi alle comunicazioni realizzate su reti elettroniche, fra cui l’accesso a fini di indagine su reati, devono soddisfare, ai sensi dell’articolo 15 della direttiva e-privacy, i requisiti che giustificano un’ingerenza nel diritto alla protezione dei dati sancito dall’articolo 8, para- grafo 2, della CEDU e confermato dalla Carta dei diritti fondamentali dell’UE agli articoli 8 e 52. Tali accessi possono avvenire allo scopo di indagare su reati.

Gli emendamenti apportati nel 2009 alla direttiva relativa alla vita privata e alle comunicazioni[918] elettroniche hanno introdotto quanto segue:

• le restrizioni all'invio di messaggi di posta elettronica a fini di marketing diretto sono state estese agli SMS, ai servizi di messaggeria multimediali e ad altri tipi di applicazioni simili; i messaggi di posta elettronica a fini di promozione commerciale sono vietati a meno che non sia stato ottenuto il consenso preventivo. Senza tale consenso, possono essere contattati con messaggi di posta elettronica a fini di promozione commerciale solo i cli- enti già acquisiti, qualora abbiano messo a disposizione il proprio indirizzo di posta elettronica e non abbiano espresso obiezioni.

• è stato imposto agli Stati membri l'obbligo di prevedere mezzi di ricorso contro le violazioni del divieto di inviare comunicazioni indesiderate[919].

• l'inserimento di marcatori («cookies»), software che controllano e regis- trano le azioni di un utente informatico, non è più consentito senza il con- senso dell'utente stesso. La legislazione nazionale dovrebbe disciplinare in maniera più dettagliata le modalità di espressione e di acquisizione del con- senso per garantire una protezione sufficiente[920].

In caso di violazione dei dati a motivo di un accesso non autorizzato, di per- dita o di distruzione di dati, l’autorità di controllo competente deve esserne

informata immediatamente. Gli abbonati devono essere informati qualora tale violazione dei dati possa arrecare loro un possibile danno[921].

La direttiva sulla conservazione dei dati[922] imponeva ai fornitori di servizi di comunicazione di conservare i metadati. Essa è, tuttavia, stata annullata dalla CGUE (per maggiori dettagli, cfr. sezione 8.3).

Prospettiva

Nel gennaio 2017, la Commissione europea ha adottato una nuova proposta di regolamento sull'e-privacy, in sostituzione della vecchia direttiva e-privacy. L'obiettivo rimarrebbe la tutela dei «diritti e delle libertà fondamentali delle persone fisiche e giuridiche per quanto attiene alla fornitura e all'uso di servizi di comunicazione elettronica, in particolare il diritto al rispetto della vita pri- vata e delle comunicazioni nonché la tutela delle persone fisiche in merito al trattamento dei dati personali», garantendo al contempo la libera circolazione dei dati di comunicazione elettronica e dei servizi di comunicazione elettron- ica all'interno dell'Unione[923]. Mentre il regolamento generale sulla protezione dei dati riguarda principalmente l'articolo 8 della Carta dei diritti fondamen- tali dell'UE, il regolamento proposto mira a integrare l'articolo 7 della Carta nel diritto derivato dell'UE.

Il regolamento adeguerà le disposizioni della precedente direttiva alle nuove tecnologie e alla realtà del mercato e creerà un quadro completo e coerente con il regolamento generale sulla protezione dei dati. In tal senso, il regola- mento sulla e-privacy costituirebbe una *lex specialis* rispetto al regolamento generale sulla protezione dei dati, che verrebbe adattato ai dati delle comu- nicazioni elettroniche che costituiscono dati personali. Il nuovo regolamento

riguarda il «trattamento dei dati delle comunicazioni elettroniche», compresi il contenuto delle comunicazioni elettroniche e i metadati che non sono neces- sariamente dati personali. L’ambito di applicazione territoriale è limitato all’UE, anche quando i dati ottenuti nell’UE vengono trattati al di fuori del territorio della stessa, e si estende ai fornitori di servizi di comunicazione «over-the-top», segnatamente ai fornitori di servizi che distribuiscono contenuti, servizi o applicazioni tramite Internet, senza il coinvolgimento diretto di un operatore di rete o di un fornitore di servizi Internet (ISP). Esempi di tali fornitori includono Skype (chiamate vocali e video), WhatsApp (messaggistica), Google (ricerca), Spotify (musica) o Netflix (contenuti video). Al nuovo regolamento si applicher- ebbero i meccanismi di attuazione del regolamento generale sulla protezione dei dati.

L’adozione del regolamento sulla e-privacy è prevista entro il 25 maggio 2018, data entro la quale il regolamento generale sulla protezione dei dati sarà appli- cabile in tutti e 28 gli Stati membri. Tuttavia, ciò è subordinato all’accordo sia del Parlamento europeo, sia del Consiglio[924].

9.2. Dati relativi al rapporto di lavoro

- La raccomandazione del CdE sul trattamento dei dati in ambito lavorativo con- tiene norme specifiche sulla protezione dei dati nei rapporti di lavoro.

- Nel regolamento generale sulla protezione dei dati, i rapporti di lavoro sono specificamente richiamati solo nel contesto del trattamento dei dati sensibili.

- La validità del consenso, che deve essere libero, come base giuridica per il trat- tamento dei dati relativi ai dipendenti può essere opinabile, dato lo squilibrio economico esistente fra il datore di lavoro e il dipendente. Le circostanze del con- senso devono essere valutate attentamente.

Il trattamento dei dati nell'ambito dei rapporti di lavoro è soggetto alla nor- mativa generale dell'UE in materia di protezione dei dati personali. Tuttavia, un regolamento[925] tratta specificamente, tra l'altro, della protezione del tratta- mento dei dati personali da parte delle istituzioni europee nell'ambito dei rap- porti di lavoro. Nel regolamento generale sulla protezione dei dati, i rapporti di lavoro sono specificamente richiamati nell'articolo 9, paragrafo 2, che stabilisce che i dati personali possono essere trattati per assolvere gli obblighi ed eserci- tare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro.

Ai sensi del regolamento generale sulla protezione dei dati, il dipendente dovrebbe essere messo in grado di distinguere chiaramente rispetto a quali dati intende prestare liberamente il consenso al trattamento/conservazione dei dati e le finalità per le quali essi vengono conservati. I dipendenti dovreb- bero altresì essere informati dei loro diritti e circa il periodo di conservazione dei dati, prima che possa essere fornito il consenso. Se la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le lib- ertà delle persone fisiche, il datore di lavoro deve comunicare la violazione al dipendente. L'articolo 88 del regolamento permette agli Stati membri di pre- vedere norme più specifiche per assicurare la protezione dei diritti e delle lib- ertà dei dipendenti

con riguardo ai loro dati personali nell’ambito dei rapporti di lavoro.

Esempio: nella causa *Worten,*[926] i dati comprendevano un registro dell’orario di lavoro in cui comparivano i periodi di lavoro giornaliere e i riposi quotidiani, che costituiscono dati personali. Il diritto nazionale può obbligare un datore di lavoro a mettere i registri dell’orario di lavoro a disposizione delle autorità nazionali competenti in materia di vigilanza sulle condizioni di lavoro. Questo consentirebbe un accesso immediato ai dati personali pertinenti Tuttavia, l’accesso ai dati personali è necessario per consentire all’autorità nazionale di esercitare vigilanza sulla normativa in materia di condizioni di lavoro[927].

Per quanto riguarda il CdE, la raccomandazione sul trattamento dei dati in ambito lavorativo è stata emanata nel 1989 ed è stata riveduta nel 2015[928]. Essa riguarda il trattamento dei dati personali per scopi di lavoro nel settore sia privato che pubblico. Il trattamento deve rispettare determinati principi e restrizioni, come il principio di trasparenza e la consultazione dei rappresent- anti dei dipendenti prima di introdurre sistemi di sor veglianza sul posto di lavoro. La raccomandazione stabilisce inoltre che i datori di lavoro devono applicare misure preventive, come filtri, anziché controllare l'utilizzo di Internet da parte dei dipendenti.

Un'indagine sui problemi più comuni relativi alla protezione dei dati e specifici del contesto lavorativo è reperibile in un documento di lavoro del Gruppo di lavoro articolo 29[929]. Il Gruppo di lavoro ha analizzato l'importanza del con- senso come base giuridica per il trattamento dei dati in ambito lavorativo[930]. Essa ha constatato che lo squilibrio economico tra il datore di lavoro che chiede il consenso e il lavoratore che lo presta solleva spesso dubbi sul fatto che il consenso sia stato dato o meno liberamente. Le circostanze nelle quali il consenso viene fatto valere come base giuridica per il trattamento dei dati dovrebbero, pertanto, essere considerate attentamente in sede di valutazione della validità del consenso in ambito lavorativo.

Un problema comune concernente la protezione dei dati nel tipico ambiente di lavoro attuale è determinare fino a che punto il controllo delle comunicazioni elettroniche dei dipendenti sul posto di lavoro sia legittimo. Si sostiene spesso che questo problema può essere facilmente risolto vietando l'uso privato dei mezzi di comunicazione sul lavoro. Tale divieto generale, tuttavia, potrebbe essere sproporzionato e non realistico. Le sentenze della Corte EDU *Copland c. Regno Unito* e *Bărbulescu c. Romania* assumono particolare rilievo in questo contesto.

Esempio: nella causa *Copland c. Regno Unito*[931], l'uso del telefono, della posta elettronica e di Internet da parte di una dipendente di un college è stato controllato in segreto per accertare se stesse facendo un uso eccessivo delle strutture del college per scopi personali. La Corte EDU ha statuito che le telefonate dal luogo di lavoro erano coperte dai concetti di vita privata e di corrispondenza. Pertanto, le telefonate e i messaggi di posta elettronica inviati dal lavoro, così come le informazioni derivanti dal monitoraggio dell'uso personale di Internet, erano protetti ai sensi dell'articolo 8 della CEDU. Nel caso della ricorrente, non esistevano disposizioni che regolamentassero le circostanze nelle quali i datori di lavoro potevano controllare l'uso del telefono, della posta elettronica e di Internet da parte dei dipendenti. Pertanto, l'ingerenza non era conforme alla legge. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Esempio: nella causa *Bărbulescu c. Romania*,[932] il ricorrente era stato licenziato per aver utilizzato il servizio Internet nel suo luogo di lavoro durante l'orario di lavoro, in violazione del regolamento interno. Il datore di lavoro aveva controllato le sue comunicazioni. Le registrazioni, che mostravano messaggi di natura puramente privata, erano state prodotte dinanzi ai tribunali nazionali. Ritenendo applicabile l'articolo 8, la Corte EDU ha

lasciato aperta la questione se le disposizioni restrittive del datore di lavoro lasciassero al richiedente un'aspettativa ragionevole in materia di vita privata, ma ritenuto, in ogni caso, che le istruzioni di un datore di lavoro non potessero ridurre a zero l'esercizio della vita privata sociale sul luogo di lavoro.

Quanto agli argomenti sul merito, agli Stati contraenti doveva essere accordato un ampio margine di valutazione per stimare la necessità di adottare un quadro giuridico a disciplina delle condizioni in cui un datore di lavoro può regolamentare le comunicazioni di natura non professionale, elettroniche o altro, dei propri dipendenti sul luogo di lavoro. Nondimeno, le autorità nazionali dovevano garantire che l'introduzione da parte di un datore di lavoro di misure per controllare la corrispondenza e altre comunicazioni, indipendentemente dalla por tata e dalla durata di tali misure, fosse accompagnata da adeguate e sufficienti garanzie contro gli abusi. La proporzionalità e le garanzie procedurali contro l'arbitrarietà erano essenziali e la Corte EDU ha individuato una serie di fattori pertinenti nelle

circostanze del caso. Essi comprendevano, tra l’altro, l’estensione del controllo da parte del datore di lavoro e il grado di intrusione nella vita privata del dipendente, le conseguenze per quest’ultimo e se fossero state fornite garanzie adeguate. Inoltre, le autorità nazionali dovevano garantire che il lavoratore, le cui comunicazioni erano state controllate, avesse accesso ad un mezzo di ricorso dinanzi a un organo giurisdizionale competente a statuire, almeno in sostanza, sul rispetto dei criteri menzionati e sulla legittimità delle misure contestate.

In questo caso, la Corte EDU ha rilevato una violazione dell’articolo 8, perché le autorità nazionali non avevano protetto in maniera adeguata il diritto del ricorrente al rispetto della sua vita privata e della sua corrispondenza e, di conseguenza, non avevano trovato un equo equilibrio tra gli interessi in gioco.

Ai sensi della raccomandazione del CdE relativa alla protezione dei dati utiliz- zati per scopi di lavoro, i dati personali raccolti per scopi lavorativi dovrebbero essere ottenuti direttamente dal singolo dipendente.

I dati personali raccolti a fini di assunzione devono essere limitati alle informazioni necessarie per valutare l’idoneità dei candidati e le loro prospet- tive di carriera.

La raccomandazione menziona specificamente anche i dati raccolti a fini di val- utazione relativi alla produttività o al potenziale dei singoli dipendenti. I dati valutativi devono basarsi su valutazioni eque e imparziali e non devono essere formulati in modo da risultare offensivi. Ciò è richiesto in forza dei principi di correttezza del trattamento dei dati personali e di esattezza degli stessi.

Un aspetto specifico del diritto in materia di protezione dei dati nel rapporto datore di lavoro-dipendente è il ruolo dei rappresentanti dei lavoratori. Tali rap- presentanti possono venire in possesso dei dati personali dei dipendenti solo nella misura in cui ciò sia necessario per consentire loro di rappresentare gli interessi dei lavoratori o se tali dati sono necessari per soddisfare o sorvegliare la conformità agli obblighi previsti dai contratti collettivi.

I dati personali sensibili raccolti per scopi relativi al rapporto di lavoro pos- sono essere trattati solo in casi particolari e nel rispetto di garanzie stabilite dalla legislazione nazionale. I datori di lavoro possono chiedere ai dipendenti o ai candidati informazioni sul loro stato di salute e possono sot toporli a

esame medico soltanto se necessario per accertarne l'idoneità all'impiego, soddisfare esigenze di medicina preventiva, salvaguardare gli interessi vitali dell'interessato o di altri dipendenti e persone fisiche, consentire il riconosci- mento delle prestazioni sociali o rispondere a richieste giudiziarie. I dati relativi alla salute non possono essere raccolti da fonti diverse dal dipendente interes- sato, tranne quando sia stato acquisito il suo consenso esplicito e informato o quando lo preveda la normativa nazionale.

Secondo la raccomandazione relativa alla protezione dei dati utilizzati per scopi di lavoro, i dipendenti dovrebbero essere informati sulla finalità del trat- tamento dei loro dati personali, sulla tipologia di dati personali raccolti, sugli organi ai quali i dati sono regolarmente comunicati nonché sulla finalità e sul fondamento giuridico di tali comunicazioni. Sul posto di lavoro è possibile accedere alle comunicazioni elettroniche solo per motivi di sicurezza o per altri motivi legittimi, e tale accesso è consentito solo dopo che i dipendenti sono stati informati del fatto che il datore di lavoro può avere accesso a questo tipo di comunicazione.

I lavoratori devono avere il diritto di accesso ai propri dati in ambito lavora- tivo nonché il diritto di rettifica o cancellazione. In caso di trattamento di dati relativi a una valutazione, i lavoratori devono inoltre avere il diritto di contes- tare tale

valutazione. Tuttavia, questi diritti possono essere temporaneamente limitati in caso di indagini interne. Se a un lavoratore sono negati l'accesso, la rettifica o la cancellazione di dati personali in ambito lavorativo, la legislazione nazionale deve prevedere procedimenti appropriati per contestare tale rifiuto.

9.3. Dati sanitari

- I dati sanitari sono dati sensibili e pertanto godono di una protezione specifica.

I dati personali concernenti la salute dell'interessato sono qualificati dati sen- sibili ai sensi dell'articolo 9, paragrafo 1, del regolamento generale sulla pro- tezione dei dati e dell'articolo 6 della Convenzione n. 108 modernizzata. Di conseguenza i dati relativi alla salute sono soggetti a un regime di trattamento

più rigoroso rispetto ai dati non sensibili. Il regolamento generale sulla protezi- one dei dati vieta il trattamento dei «dati personali relativi alla salute» (intesi come «tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso»[933], compresi i dati genetici e i dati biometrici, salvo se autorizzato dall'articolo 9, paragrafo 2. Entrambi i tipi di dati sono stati aggiunti all'elenco delle «categorie particolari di dati»[934].

Esempio: nella causa *Z c. Finlandia*,[935] l'ex marito della ricorrente, che aveva contratto il virus dell'HIV, aveva commesso una serie di reati di natura sessuale. Successivamente era stato accusato di omicidio colposo per avere esposto consapevolmente le sue vittime al rischio di infezione da HIV. Il giudice nazionale aveva disposto un periodo di riservatezza di 10 anni per la sentenza integrale e i documenti relativi alla causa, malgrado la ricorrente avesse chiesto la concessione di un periodo di riservatezza più lungo. La corte d'appello aveva respinto tali richieste con una sentenza nella quale apparivano i nomi completi della ricorrente e dell'ex marito. La Corte EDU ha statuito che l'ingerenza non era da ritenersi necessaria in una società democratica, dal momento che la protezione dei dati sanitari era di fondamentale importanza per il godimento del diritto

al rispetto della vita privata e familiare, in particolare per quanto riguarda le informazioni sulle infezioni da HIV, data la stigmatizzazione di questa condizione in numerose società. Pertanto, la Corte ha concluso che il fatto di consentire l'accesso alla sentenza della corte d'appello, che descriveva l'identità e la condizione sanitaria della ricorrente, dopo un periodo di soli 10 anni dalla sua pronuncia, costituiva una violazione dell'articolo 8 della CEDU.

Nell'ambito del diritto dell'UE, l'articolo 9, paragrafo 2, lettera h), del regola- mento generale sulla protezione dei dati consente il trat tamento dei dati sanitari quando ciò sia necessario alla prevenzione o alla diagnostica medica,

alla somministrazione di cure o alla gestione di centri di cura. Il trattamento è autorizzato, tuttavia, solo quando è effettuato da un operatore professioni- sta in campo sanitario soggetto al segreto professionale o da un’altra persona parimenti soggetta a un obbligo equivalente.

Nell’ambito del diritto del CdE, la raccomandazione del CdE relativa alla pro- tezione dei dati sanitari del 1997 applica in modo più dettagliato i principi della Convenzione n. 108 al trattamento di dati personali nel settore medico[936]. Le norme proposte sono in linea con quelle del regolamento generale sulla pro- tezione dei dati per quanto riguarda gli scopi legittimi del trattamento dei dati sanitari, il necessario obbligo del segreto professionale per le persone che usano dati relativi alla salute e i diritti degli interessati alla trasparenza e all’accesso, alla rettifica e alla cancellazione. Inoltre, i dati sanitari trattati legit- timamente da operatori sanitari professionisti non possono essere trasmessi alle autorità di contrasto a meno che non siano previste «sufficienti garanzie per impedire una divulgazione non coerente con il rispetto della [...] vita privata sancito dall’articolo 8 della CEDU»[937]. Il diritto nazionale deve altresì essere «formulato con sufficiente precisione e prevedere una protezione legale ade- guata contro l’arbitrarietà»[938].

Inoltre, la raccomandazione relativa alla protezione dei dati sanitari con- tiene disposizioni specifiche sui dati sanitari di bambini non nati e di per- sone inabili nonché sul trattamento di dati genetici. La ricerca scientifica è esplicitamente riconosciuta come motivo per conservare i dati per un peri- odo di tempo più lungo del necessario, sebbene in tal caso sia richiesta di solito l'a nonimiz zazione. L'articolo 12 della raccoma ndazione relativa ai dati sanitari propone l'adozione di regolamenti dettagliati per le situazioni in cui i ricercatori necessitano di dati personali e i dati anonimiz zati sono insufficienti.

La pseudonimizzazione può rappresentare uno strumento appropriato per soddisfare le esigenze scientifiche e tutelare, nel contempo, gli interessi dei

pazienti interessati. Il concetto di pseudonimizzazione nel contesto della pro- tezione dei dati è illustrato in modo più dettagliato nella sezione 2.1.1.

La raccomandazione del CdE del 2016 sui dati risultanti da prove genetiche si applica anche al trattamento dei dati nel settore medico[939]. Questa raccoman- dazione è di grande impor tanza per la sanità elettronica, dove le TIC sono utilizzate per facilitare l'assistenza medica. Un esempio è la trasmissione dei risultati di un test di paternità di un paziente da un operatore sanitario a un altro. Questa raccomandazione mira a tutelare i diritti delle persone i cui dati personali sono trattati a fini assicurativi contro i rischi per la salute, l'integrità fisica, l'età o il decesso di una persona. Gli assicuratori devono giustificare il trattamento dei dati relativi alla salute, che deve essere proporzionato alla natura e all'importanza del rischio considerato. Il trattamento di questo tipo di dati è subordinato al consenso dell'interessato. Gli assicuratori dovrebbero inoltre prevedere garanzie per la conservazione dei dati personali relativi alla salute.

La sperimentazione clinica, che comprende la valutazione degli effetti di nuovi medicinali sui pazienti in ambienti di ricerca documentati, ha notevoli implica- zioni in termini di protezione dei dati. La sperimentazione clinica di medicinali per uso

umano è disciplinata dal regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE (regolamento sulla sperimentazione clinica)[940]. Gli elementi essenziali del regolamento sulla sperimentazione clinica sono i seguenti:

- una procedura di domanda semplificata mediante il portale UE[941];

- scadenze per la valutazione della domanda di sperimentazione clinica[942],

- un comitato etico partecipante alla valutazione a norma del diritto degli Stati membri (e del diritto europeo che definisce i periodi di riferimento)[943]; e
- maggiore trasparenza della sperimentazione clinica e dei relativi risultati[944]. Il regolamento generale sulla protezione dei dati precisa che ai fini del con-
senso alla partecipazione alle attività di ricerca scientifica nell'ambito delle
sperimentazioni cliniche si applica il regolamento (UE) n. 536/2014[945].

Molte altre iniziative legislative e di altro tipo in materia di dati personali nel settore sanitario sono in corso a livello di UE[946].

Cartelle cliniche elettroniche

Le cartelle cliniche elettroniche sono definite come «documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, pas- sato e presente di un individuo in forma elettronica, che consenta la pronta disponibilità di tali dati per cure mediche e altri fini strettamente collegati»[947]. Le cartelle cliniche elettroniche sono versioni elettroniche degli antecedenti sanitari dei pazienti e possono includere dati clinici relativi a tali persone, quali anamnesi, problemi e patologie, farmaci e trattamenti, nonché risultati e relazioni di esami e

laboratorio. Tali fascicoli elettronici, che possono vari- are da interi fascicoli a semplici estratti o riassunti, sono accessibili al medico di medicina generale, al farmacista e ad altri operatori sanitari. Il concetto di
«sanità elettronica» riguarda anche queste cartelle cliniche.

Esempio: il signor A ha stipulato una polizza assicurativa con la società B, l'assicuratore. Quest'ultimo raccoglierà alcune informazioni attinenti alla salute di A, come questioni sanitarie o malattie in corso. L'assicuratore

dovrebbe conservare i dati personali attinenti alla salute di A separatamente dagli altri dati. Egli deve inoltre conservare i dati personali attinenti alla salute separatamente dagli altri dati personali. Questo significa che solo l'addetto al fascicolo di A avrà accesso ai dati attinenti alla salute di A.

Tuttavia, le cartelle cliniche elettroniche sollevano alcune questioni in mate- ria di protezione dei dati, quali la loro accessibilità, la corretta conservazione e l'accesso da parte dell'interessato.

Oltre alle cartelle cliniche elettroniche, il 10 aprile 2014 la Commissione euro- pea ha pubblicato un Libro verde sulla sanità mobile (mHealth), ritenendo la mHealth un settore emergente e in rapido sviluppo, in grado di contribuire a trasformare l'assistenza sanitaria, e di aumentarne l'efficienza e la qualità. Il termine fa riferimento alla pratica della medicina e della sanità pubblica sup- portata da dispositivi mobili, quali telefoni cellulari, dispositivi per il monitor- aggio dei pazienti, computer palmari e altri dispositivi senza fili, nonché alle applicazioni (ad esempio, le applicazioni per il benessere) che possono connet- tersi a dispositivi medici o sensori[948]. Il libro verde individua i rischi correlati al diritto alla protezione dei dati personali, che la mHealth potrebbe comportare e stabilisce che, data l'estrema delicatezza dei dati sanitari, lo sviluppo dovrebbe offrire garanzie di sicurezza specifiche e

idonee per i dati dei pazienti, come la crittografia, e meccanismi adeguati di autenticazione del paziente al fine di attenuare i rischi di sicurezza. Il rispetto delle norme sulla protezione dei dati personali, compreso l'obbligo di informare gli interessati, la sicurezza dei dati e il principio di liceità del trattamento dei dati personali sono essenziali per creare fiducia nelle soluzioni di mHealth[949]. A tale scopo l'industria ha redatto un progetto di codice di condotta, basato su contributi provenienti da una plu- ralità di parti interessate, tra cui rappresentanti con competenze in materia di protezione dei dati, autoregolamentazione e coregolamentazione, TIC e in ambito sanitario[950]. Al momento della stesura del manuale, il progetto di codice di condotta era stato sottoposto all'esame del Gruppo di lavoro articolo 29 per la protezione dei dati, in attesa della sua approvazione formale.

9.4. Trattamento di dati personali a fini statistici e di ricerca

- I dati raccolti a fini di ricerca statistica, scientifica o storica non possono essere usati per nessun altro scopo.
- I dati raccolti in modo legittimo per qualsiasi finalità possono essere utilizzati ulteriormente a fini di ricerca statistica, scientifica o storica, a condizione che siano predisposte garanzie adeguate. A tal fine, l'anonimizzazione o la pseudoni- mizzazione prima della trasmissione dei dati a terzi possono offrire tali garanzie.

Il diritto dell'UE consente il trattamento dei dati a fini statistici o per finalità di ricerca scientifica o storica, a condizione che siano previste garanzie adeguate per i diritti e le libertà degli interessati. Queste possono comprendere la pseu- donimizzazione[951]. Il diritto dell'Unione o il diritto nazionale possono preve- dere talune deroghe ai diritti degli interessati, se tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità legit- tima della ricerca[952]. Possono essere introdotte deroghe al diritto di accesso, al diritto di

rettifica, al diritto di limitazione del trattamento e al diritto di oppo- sizione dell'interessato.

Sebbene i dati raccolti in modo lecito da un titolare del trattamento per qual- siasi scopo possano essere riutilizzati da tale titolare per i propri fini di ricerca statistica, scientifica o storica, i dati dovrebbero essere anonimizzati o sot- toposti a misure quali la pseudonimizzazione, a seconda del contesto, prima di essere trasmessi a terzi per fini di ricerca statistica scientifica o storica, a meno che l'interessato vi abbia acconsentito, o sia specificamente previsto dal diritto nazionale. Diversamente dai dati anonimi, i dati sottoposti a pseudonimizzazi- one restano assoggettati al regolamento generale sulla protezione dei dati[953].

Il regolamento accorda pertanto un trattamento speciale alla ricerca per quanto riguarda le norme generali sulla protezione dei dati, per evitare restrizioni allo sviluppo della ricerca e garantire il rispetto dell'obiettivo di istituire uno

spazio europeo della ricerca ai sensi dell'articolo 179 del TFUE. Esso prevede un'interpretazione in senso lato del trattamento dei dati personali per final- ità di ricerca scientifica, compresi lo sviluppo tecnologico e la dimostrazione, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata da privati. Esso riconosce inoltre l'importanza dell'iscrizione dei dati in registri a fini di ricerca e la possibile difficoltà di individuare pienamente la finalità successiva del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati[954]. Per questa ragione, il regolamento consente il trattamento dei dati per tali scopi senza il consenso dell'interessato, a condizione che ven- gano poste in essere le garanzie del caso.

Un esempio importante dell'utilizzo dei dati a fini statistici sono le statistiche ufficiali ottenute dagli istituti statistici nazionali e dell'UE ai sensi del diritto nazionale e dell'UE sulle statistiche ufficiali. In virtù di tali norme, i cittadini e le imprese sono di solito obbligati a comunicare dati alle pertinenti autorità statistiche. I funzionari degli istituti statistici sono vincolati da specifici obbli- ghi di segreto professionale che devono essere osservati correttamente, dal momento che risultano essenziali per l'esistenza di un elevato livello di fiducia dei cittadini, necessario affinché i dati siano messi a disposizione delle autorità statistiche[955].

Il regolamento (CE) n. 223/2009 sulle statistiche europee (regolamento sulle statistiche europee) contiene norme essenziali per la protezione dei dati in materia di statistiche ufficiali; pertanto, anch’esso può essere considerato rile- vante per quanto riguarda le disposizioni sulle statistiche ufficiali a livello nazi- onale[956]. Il regolamento mantiene il principio secondo cui l’attività statistica ufficiale necessita di una base giuridica sufficientemente chiara[957].

Esempio: nella causa *Huber c. Bundesrepublik Deutschland*[958], un uomo d'affari austriaco che si era stabilito in Germania lamentava il fatto che la raccolta e la conservazione dei dati personali di cittadini stranieri da parte delle autorità tedesche in un registro centrale (AZR) anche a fini statistici violava i suoi diritti ai sensi della direttiva sulla tutela dei dati. Considerando che la direttiva 95/46/CE mira a garantire un livello di protezione dei dati equivalente in tutti gli Stati membri, la CGUE ha ritenuto che, per garantire un elevato grado di tutela nell'UE, la nozione di necessità di cui all'articolo 7, lettera e), non può avere un contenuto variabile in funzione degli Stati membri. Pertanto, si tratta di una nozione autonoma del diritto dell'UE, e deve essere interpretata in maniera tale da rispondere pienamente alla finalità della direttiva 95/46. La CGUE, osservando che per fini statistici dovrebbero essere richieste solo informazioni anonime, ha statuito che il registro tedesco non era compatibile con il requisito di necessità di cui all'articolo 7, lettera e).

Nell'ambito del CdE, l'ulteriore trattamento dei dati è consentito a fini di ricerca scientifica, storica o statistica qualora sia nel pubblico interesse, e deve essere assoggettato a garanzie adeguate[959]. I diritti degli interessati possono essere limitati anche per il trattamento dei dati a fini statistici, a condizione che non esista un rischio riconoscibile di violazione dei loro diritti e delle loro libertà[960].

La raccomandazione sui dati statistici emanata nel 1997 concerne la realizzazi- one di statistiche nei settori pubblico e privato[961].

I dati raccolti da un titolare del trattamento a fini statistici non possono essere usati per nessun altro scopo. I dati raccolti per scopi non statistici sono utiliz- zabili ulteriormente a fini statistici. La raccomandazione sui dati statistici con- sente anche la comunicazione dei dati a terzi a condizione che ciò avvenga solo per fini statistici. In tali casi, le parti dovrebbero concordare e formalizzare per iscritto la portata dell'ulteriore uso legittimo a fini statistici. Poiché questo non può sostituire il consenso dell'interessato, ove necessario, la legislazione nazi- onale deve prevedere garanzie appropriate per minimizzare i rischi di abuso di

dati personali, quali l'obbligo di anonimizzare o pseudonimizzare i dati prima della trasmissione.

I professionisti della ricerca statistica devono essere vincolati da speciali obbli- ghi di segreto professionale, come avviene di solito per le statistiche ufficiali, ai sensi della legislazione nazionale. Questo deve valere anche per gli intervista- tori e altri addetti alla raccolta dei dati personali, se impegnati nella raccolta dei dati presso gli interessati o altre persone.

Se un'indagine statistica che si avvale di dati personali non è autorizzata dalla legge, per gli interessati potrebbe essere necessario acconsentire all'uso dei loro dati per renderla legittima, o avere la possibilità di obiettarvi. Se i dati personali sono raccolti a fini statistici dagli intervistatori, questi ultimi devono essere chiaramente informati circa l'obbligatorietà o meno della divulgazione dei dati ai sensi della legislazione nazionale.

Quando un'indagine statistica non può essere realizzata sulla base di dati anonimi, e sono necessari dati personali, i dati raccolti per quello scopo devono essere resi anonimi il prima possibile. I risultati dell'indagine statistica non devono, per lo meno, consentire l'identificazione di qualsiasi interessato, a meno che ciò non presenti chiaramente alcun rischio.

Dopo la conclusione dell’analisi statistica, i dati personali usati dovrebbero essere cancellati o anonimizzati. In questi casi, la raccomandazione sui dati statistici suggerisce di conservare i dati identificativi separatamente dagli altri dati personali. Questo significa, ad esempio, che la chiave di cifratura o l’elenco contenente i sinonimi di identificazione deve essere conservata separatamente dagli altri dati.

9.5. Dati finanziari

- Benché i dati finanziari non siano considerati dati sensibili ai sensi della Conven- zione n. 108 modernizzata o del regolamento generale sulla protezione dei dati, il loro trattamento necessita di particolari garanzie per garantirne l’esattezza e la sicurezza.

• I sistemi di pagamento elettronico necessitano in modo particolare di una protezione dei dati integrata, ossia della protezione della vita privata fin dalla pro- gettazione e della protezione per impostazione predefinita.

• Particolari problemi di protezione dei dati possono sorgere in questo settore dall'esigenza di attuare appropriati meccanismi di autenticazione.

Esempio: nella causa *Michaud c. Francia*[962], il ricorrente, un avvocato francese, ha contestato l'obbligo impostogli dalla legge francese di comunicare eventuali sospetti su possibili attività di riciclaggio di denaro da parte dei clienti. La Corte EDU ha osservato che l'imposizione agli avvocati dell'obbligo di comunicare alle autorità amministrative informazioni sul conto di un'altra persona, ottenute attraverso scambi professionali costituiva un'ingerenza nel diritto degli avvocati al rispetto della propria corrispondenza e vita privata ai sensi dell'articolo 8 della CEDU, poiché quel concetto si estendeva alle attività di natura professionale o commerciale. Tuttavia, l'ingerenza era conforme alla legge e perseguiva un obiettivo legittimo, ossia la prevenzione di disordini e di reati. Poiché gli avvocati sono soggetti all'obbligo di

comunicare attività sospette solo in circostanze molto specifiche, la Corte EDU ha statuito che l'obbligo era proporzionato ed ha concluso che non vi era stata alcuna violazione dell'articolo 8.

Esempio: nella causa *M.N. e a. c. San Marino*[963], il ricorrente, un cittadino italiano, aveva concluso un accordo con una società fiduciaria sotto inchiesta. Ciò significava che la società era oggetto di provvedimenti di perquisizione e sequestro di copie della documentazione (elettronica). Il ricorrente aveva presentato ricorso dinanzi al tribunale di San Marino, sostenendo che tra lui e i presunti reati non vi era alcun legame. Tuttavia, il giudice aveva dichiarato il ricorso irricevibile, dal momento che il ricorrente non era una «parte interessata». La Corte EDU ha ritenuto il ricorrente sensibilmente svantaggiato con riferimento alla tutela giudiziaria rispetto ad una «parte interessata», tuttavia, i suoi dati restavano soggetti alle operazioni di ricerca e sequestro. Pertanto, la Corte ha ritenuto che vi era stata violazione dell'articolo 8.

Esempio: nella causa *G.S.B. c. Svizzera*[964], i dati bancari del ricorrente erano stati trasmessi alle autorità fiscali statunitensi sulla base dell'accordo di cooperazione amministrativa tra la Svizzera e gli Stati Uniti. La Corte EDU ha ritenuto che la trasmissione non violasse l'articolo 8 della CEDU, poiché l'ingerenza nel diritto del ricorrente alla vita privata era prevista dalla legge, perseguiva un obiettivo legittimo ed era proporzionata all'interesse pubblico in questione.

L'applicazione del quadro giuridico generale per la protezione dei dati (prevista dalla Convenzione n. 108) al contesto dei pagamenti è stata sviluppata dal CdE nella raccomandazione Rec(90)19 del 1990[965]. Tale raccomandazione chiarisce la portata della raccolta e dell'uso legittimi dei dati nell'ambito dei pagamenti, specialmente mediante carte di pagamento. Essa fornisce inoltre ai legislatori nazionali raccomandazioni dettagliate sulle disposizioni in materia di comunica- zione a terzi dei dati relativi a pagamenti, sui limiti temporali della conservazi- one dei dati, sulla trasparenza, sulla sicurezza dei dati e i flussi transfrontalieri degli stessi nonché in materia di controllo e di mezzi di ricorso. Il CdE ha inol- tre formulato un parere sul trasferimento dei dati fiscali[966], che contiene rac- comandazioni e indicazioni sulle questioni da considerare nel trattare il trasferi- mento di dati fiscali.

La Corte EDU consente la trasmissione dei dati finanziari (e in particolare dei dettagli del conto bancario di una persona) ai sensi dell'articolo 8 della CEDU, ove sia prescritta dalla legge, persegua uno scopo legittimo e sia proporzionata all'interesse pubblico in questione[967].

Nell'ambito del diritto dell'UE, i sistemi di pagamento elettronico che compor- tano il trattamento dei dati personali devono essere conformi al regolamento generale sulla protezione dei dati. Pertanto, tali sistemi devono garantire la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita. La protezione dei dati fin dalla progettazione obbliga il titolare del trattamento a mettere in atto misure tecniche e organizzative adeguate al fine

di applicare i principi di protezione dei dati. Protezione dei dati per impostazi- one predefinita significa che il titolare del trattamento deve garantire che siano trattati per impostazione predefinita solo i dati personali necessari per una finalità specifica (cfr. sezione 4.4). Per quanto riguarda i dati finanziari, la CGUE ha stabilito che i dati fiscali trasferiti possono costituire dati personali[968]. Il Gruppo di lavoro articolo 29 per la protezione dei dati ha emanato linee guida destinate agli Stati membri, che includono criteri per garantire il rispetto delle norme in materia di protezione dei dati nello scambio automatico dei dati per- sonali a fini fiscali con mezzi automatizzati[969]. Inoltre, è stata adottata una serie di strumenti giuridici per regolamentare i mercati finanziari nonché le attività degli enti creditizi e delle imprese di investimento[970]. Altri strumenti giuridici contribuiscono alle attività di contrasto dell'abuso di informazioni privilegiate e della manipolazione dei mercati[971]. I principali settori che incidono sulla protezi- one dei dati sono:

- la conservazione di registrazioni delle operazioni finanziarie;

- il trasferimento di dati personali verso paesi terzi;

- la registrazione di conversazioni telefoniche o di comunicazioni elettron- iche, compreso il potere

delle autorità competenti di richiedere le registrazioni dei dati telefonici e dei dati relativi al traffico;

- la divulgazione di informazioni personali, compresa la pubblicazione di sanzioni;

- i poteri di controllo e di indagine delle autorità competenti, comprese le ispezioni in loco e l'ingresso in locali privati per il sequestro di documenti;

- i meccanismi per la comunicazione di violazioni, vale a dire regimi di denun- cia di irregolarità e

- la cooperazione fra le autorità competenti degli Stati membri e l'Autorità europea degli strumenti finanziari e dei mercati (ESMA).

In questi settori sono affrontate specificamente anche altre questioni, fra cui la raccolta di dati sulla condizione finanziaria degli interessati[972] o sui pagamenti transfrontalieri attraverso bonifici bancari, che inevitabilmente comporta la creazione di flussi di dati personali[973].

L’era digitale, o era delle tecnologie dell’informazione, è caratterizzata dall’uso diffuso di computer, Internet e tecnologie digitali. Essa comporta la raccolta e il trattamento di grandi quantità di dati, compresi i dati personali. La raccolta e il trattamento di dati personali in un’economia globalizzata comportano un aumento dei flussi transfrontalieri di dati. Tale trattamento può apportare benefici significativi e visibili nella vita quotidiana: i motori di ricerca facilitano l’accesso a volumi considerevoli di informazioni e conoscenze, i servizi di social network consentono alle persone in tutto il mondo di comunicare, esprimere pareri e mobilitare il sostegno per cause sociali, ambientali e politiche, men- tre aziende e consumatori

beneficiano di tecniche di marketing efficaci ed effi- cienti che stimolano l'economia. Tecnologia e trattamento dei dati personali sono strumenti indispensabili anche per le autorità statali nella lotta contro la criminalità e il terrorismo. Analogamente, i megadati - la raccolta, conservazi- one e analisi di grandi quantità di informazioni per individuare modelli e preve- dere comportamenti - «possono essere fonte di grande valore per la società, permettendo di aumentare la produttività, le prestazioni del settore pubblico e la partecipazione sociale»[974].

Nonostante i suoi molteplici vantaggi, l'era digitale pone anche sfide per quanto riguarda la vita privata e la protezione dei dati, in quanto la raccolta e il trattamento di enormi quantità di informazioni personali avvengono con modalità sempre più complesse e opache. I progressi delle tecnologie hanno

portato allo sviluppo di enormi insiemi di dati che possono essere facilmente sottoposti a controlli incrociati e ulteriormente analizzati per individuare mod- elli o adottare decisioni basate su algoritmi, che possono tracciare un quadro senza precedenti del comportamento umano e della vita privata[975].

Le nuove tecnologie sono potenti e possono rivelarsi particolarmente perico- lose se cadono nelle mani sbagliate. Le autorità statali che svolgono attività di sorveglianza di massa e che possono avvalersi di tali tecnologie costituis- cono un esempio dell'impatto significativo che queste ultime possono avere sui diritti delle persone. Nel 2013, le rivelazioni di Edward Snowden sul fun- zionamento dei programmi di sorveglianza telefonica e di Internet su larga scala da parte delle agenzie di intelligence in alcuni Stati ha suscitato notevoli preoccupazioni circa i rischi che le attività di sorveglianza comportano per la vita privata, la governance democratica e la libertà di espressione. La sorveg- lianza di massa e le tecnologie che consentono l'archiviazione e il trattamento globalizzati di informazioni personali e l'accesso in blocco ai dati possono ledere l'essenza stessa del diritto alla vita privata[976]. Inoltre, possono avere un impatto negativo sulla cultura politica e un effetto dissuasivo sulla democrazia, la creatività e l'innovazione[977]. Il semplice timore che lo Stato possa costante- mente sorvegliare e analizzare il comportamento e le azioni dei cittadini può

scoraggiarli dall'esprimere le loro opinioni su talune questioni e tradursi in dif- fidenza e cautela[978]. Queste sfide hanno spinto numerose autorità pubbliche, centri di ricerca e organizzazioni della società civile ad analizzare il potenziale impatto delle nuove tecnologie sulla società. Nel 2015, il Garante europeo della protezione dei dati ha lanciato diverse iniziative volte a valutare l'impatto dei megadati e dell'Internet degli oggetti sull'etica. In particolare, il GEPD ha isti- tuito un gruppo consultivo etico che mira a «incentivare un dibattito aperto e informato sull'etica digitale, che consenta all'UE di concretizzare i benefici della

tecnologia per la società e l'economia e, al contempo, rafforzi i diritti e le lib- ertà dei singoli, in particolare i loro diritti alla vita privata e alla protezione dei dati»[979].

Il trattamento dei dati personali è anche un potente strumento nelle mani delle aziende. Oggi può rivelare informazioni dettagliate sulla situazione sanitaria o finanziaria di una persona, informazioni che vengono poi utilizzate dalle società per prendere decisioni importanti per le persone, come la determinazione del loro premio di assicurazione sanitaria o la loro affidabilità creditizia. Le tecniche di trattamento dei dati possono avere un impatto anche sui processi democrat- ici quando vengono utilizzate da politici o imprese per influenzare le elezioni, ad esempio, attraverso la «microdefinizione degli obiettivi» delle comunica- zioni agli elettori. In altre parole, se in un primo tempo la privacy era percepita come un diritto di proteggere le persone da ingerenze ingiustificate da parte delle autorità pubbliche, nell'era moderna, può anche essere minacciata dai poteri degli operatori privati. Ciò solleva interrogativi circa l'uso della tecno- logia e dell'analisi predittiva nelle decisioni che influenzano la vita quotidiana delle persone e rafforza la necessità di garantire che qualsiasi trattamento di dati personali rispetti i requisiti in materia di diritti fondamentali.

La protezione dei dati è intrinsecamente connessa ai cambiamenti tecnologici, sociali e politici. Sarebbe quindi impossibile redigere un elenco completo delle sfide future. Questo capitolo esamina alcuni settori specifici riguardanti i mega- dati, i social network e il mercato unico digitale dell'UE. Non si tratta di una valutazione esaustiva di questi settori dal punto di vista della protezione dei dati, ma piuttosto di evidenziare le molteplici interazioni possibili tra le attività umane nuove o rivedute e la protezione dei dati.

10.1. Megadati, algoritmi e intelligenza artificiale

- Innovazioni destabilizzanti nel settore delle tecnologie dell'informazione e della comunicazione stanno plasmando un nuovo stile di vita in cui le relazioni sociali,

le imprese, i servizi pubblici e privati sono interconnessi per via digitale, gen- erando in tal modo una quantità di dati sempre maggiore, molti dei quali dati personali.

- Governi, imprese e cittadini operano sempre più spesso in un'economia basata sui dati, nella quale i dati stessi sono diventati risorse preziose.

- Il concetto di megadati si riferisce sia ai dati, che alla loro analisi.

- I dati personali trattati attraverso l'analisi dei megadati sono disciplinati dalla leg- islazione dell'UE e del CdE.

- Le deroghe alle norme e ai diritti in materia di protezione dei dati sono limitate a diritti specifici e situazioni par ticolari in cui l'esercizio di un diritto risulter- ebbe impossibile o richiederebbe sforzi sproporzionati da parte dei titolari del trattamento.

- I processi decisionali interamente automatizzati sono di norma vietati, tranne in casi specifici.

- La consapevolezza e il controllo da parte dei singoli sono fondamentali per gar- antire l'applicazione dei diritti.

In questo mondo sempre più digitalizzato, ogni attività lascia una traccia digitale che può essere raccolta, trattata e valutata o analizzata. Con le nuove tecnologie di informazione e comunicazione, viene raccolta e registrata una quantità sem- pre maggiore di dati[980]. Fino a poco tempo fa, nessuna tecnologia era in grado di analizzare o valutare la massa di dati o trarne conclusioni utili. I dati erano sem- plicemente troppo numerosi per essere valutati, troppo complessi, scarsamente strutturati e in rapida evoluzione per individuare tendenze e abitudini.

10.1.1. Definizione di megadati, algoritmi e intelligenza artificiale

Megadati

Il termine «megadati» ("big data") è una parola chiave che può riferirsi a diversi concetti, a seconda del contesto. Esso comprende tipicamente «la crescente capacità tecnologica di raccogliere, trattare ed estrarre conoscenze

nuove e predittive a partire da grandi volumi, varietà e velocità dei dati»[981]. La nozione di megadati si riferisce quindi sia ai dati stessi, sia all'analisi dei dati.

Le fonti dei dati sono di vario tipo e comprendono le persone e i loro dati per- sonali, macchine o sensori, dati sul clima, immagini satellitari, immagini e video digitali, o segnali GPS. Gran parte dei dati e delle informazioni, tuttavia, è costi- tuita da dati personali, che si tratti di nomi, fotografie, indirizzi e-mail, estremi bancari, dati GPS di tracciabilità, messaggi su siti di reti sociali, informazioni cliniche o indirizzi IP di computer[982].

Per megadati si intendono anche il trattamento, l'analisi e la valutazione delle masse di dati e delle informazioni disponibili, per ottenere informazioni utili ai fini dell'analisi dei megadati. Ciò significa che i dati e le informazioni rac- colti possono essere utilizzati per scopi diversi dalle finalità iniziali, ad esem- pio andamenti statistici o servizi più personalizzati, come la pubblicità. Di fatto, laddove esistono le tecnologie per raccogliere, trattare e valutare i megadati, qualsiasi tipo di informazione può essere combinata e rivalutata: transazioni finanziarie, affidabilità creditizia, cure mediche, consumo privato, attività pro- fessionale, tracciabilità e percorsi intrapresi, uso di Internet, schede elettron- iche e smartphone, monitoraggio video o delle comunicazioni. L'analisi dei megadati

introduce una nuova dimensione quantitativa dei dati, che possono essere valutati e utilizzati in tempo reale, ad esempio, per fornire ai consuma- tori servizi personalizzati.

Algoritmi e intelligenza artificiale

L'intelligenza artificiale (IA) si riferisce all'intelligenza delle macchine che agis- cono come «agenti intelligenti». In quanto agenti intelligenti, alcuni dispositivi possono, con il supporto di software, percepire il proprio ambiente e agire in

base ad algoritmi. Il termine IA viene utilizzato quando una macchina imita funzioni «cognitive», come l'apprendimento e la soluzione di problemi, che normalmente sarebbero associate a persone fisiche[983]. Per simulare il processo decisionale, le tecnologie moderne e i software si basano su algoritmi, che i dispositivi utilizzano per prendere «decisioni automatizzate». Un algoritmo può essere descritto come una procedura in più fasi per il calcolo, il tratta- mento dei dati, la valutazione, e il ragionamento e il processo decisionale automatizzati.

Analogamente all'analisi dei megadati, l'intelligenza artificiale e il processo decisionale automatizzato che ne deriva, richiedono la raccolta e il trattamento di grandi quantità di dati. Questi dati possono provenire dal dispositivo stesso (calore dei freni, carburante, ecc.) o dall'ambiente circostante. La profilazione, per esempio, è un processo che basarsi su un processo decisionale automatiz- zato secondo modelli o fattori predeterminati.

Esempio: Profilazione e pubblicità mirata

La profilazione basata sui megadati comporta la ricerca di modelli che riflettano le «caratteristiche di un tipo di personalità», ad esempio, quando le aziende di shopping online propongono prodotti utilizzando la formula

«potrebbe interessarti anche», basandosi su informazioni raccolte dai prodotti precedentemente inseriti nel carrello di un cliente. Maggiore è la quantità di dati, più il mosaico è preciso. Lo smartphone, ad esempio, è un potente questionario che le persone compilano ad ogni utilizzo, consciamente e inconsciamente.

La psicografia moderna – scienza che studia la personalità – utilizza il metodo OCEAN, sulla base del quale determina i tipi di personalità trattati. Le dimensioni della personalità, i cosiddetti «Big Five», [ossia i cinque parametri della personalità], sono: apertura mentale (Openness: quanto la persona è aperta alla novità), coscienziosità (Conscientiousness: quanto la persona è perfezionista), l'estroversione (Extraversion: quanto la persona è socievole), amicalità (Agreeableness: quanto la persona è collaborativa)

e nevroticismo (Neurocitisism: quanto la persona è vulnerabile). Queste informazioni forniscono un profilo della persona in questione, dei suoi bisogni, dei suoi timori, del suo comportamento, ecc.. Esse vengono poi integrate da altre informazioni riguardanti la persona, ottenute da qualsiasi fonte disponibile, da intermediari di dati e social network (compresi i «like» e le fotografie pubblicati), alla musica ascoltata online, o a dati GPS e di tracciabilità.

I profili creati attraverso le tecniche di analisi dei megadati vengono successivamente messi a confronto, per individuare modelli simili e interpretare gruppi di personalità. Le informazioni sul comportamento e gli atteggiamenti di talune personalità sono, quindi, invertite. Con l'accesso ai megadati e il loro utilizzo, il test di personalità è ribaltato, sono ora le informazioni sul comportamento e l'atteggiamento a descrivere la personalità dell'individuo. Combinando le informazioni sui «like» nei social network, i dati di tracciabilità, la musica ascoltata o i film guardati, può emergere un quadro chiaro della personalità di un individuo, che consente alle aziende di comunicare pubblicità e/o informazioni su misura in funzione della
«personalità» dello stesso. Soprattutto, queste informazioni possono essere trattate in tempo reale[984].

10.1.2. Bilanciamento dei vantaggi e dei rischi dei megadati

Le moderne tecniche di trattamento dei dati possono gestire grandi masse di dati, impor tarne rapidamente di nuove, prevedere il trat tamento delle informazioni in tempo reale in termini di brevi tempi di risposta (anche nel caso di richieste complesse), prevedere la possibilità di richieste multiple e simulta- nee, e analizzare diversi tipi di informazioni (fotografie, testi o numeri). Queste innovazioni tecnologiche consentono di strutturare, trattare e valutare masse

di dati e informazioni in tempo reale[985]. Aumentando in modo esponenziale la quantità di dati disponibili e analizzati, si possono ora ottenere risultati che sarebbero impossibili da ottenere in un'analisi su scala più ridotta. I megadati hanno contribuito a sviluppare un nuovo settore di attività, nel quale possono emergere nuovi servizi per le imprese e per i consumatori. Da qui al 2020, il valore dei dati personali dei cittadini dell'UE potrebbe aumentare fino a quasi
1 000 miliardi di EUR l'anno[986]. Pertanto, i megadati possono offrire nuove opportunità risultanti dalla valutazione dei dati di massa per nuove intuizioni sociali, economiche o scientifiche, che possono avvantaggiare sia le persone, che le imprese e i governi[987].

L'analisi dei megadati può rivelare l'esistenza di modelli tra diverse fonti e insiemi di dati, che forniscono utili spunti in settori come la scienza e la medicina. È questo il caso, ad esempio, in settori quali la sanità, la sicurezza alimentare, i sistemi di trasporto intelligenti, l'efficienza energetica o la piani- ficazione urbana. Questa analisi in tempo reale delle informazioni può essere utilizzata per migliorare i sistemi sviluppati. Nel settore della ricerca, attraverso la combinazione di grandi quantità di dati e valutazioni statistiche possono essere acquisite nuove conoscenze, soprattutto nelle discipline in cui, fino ad oggi, grandi masse di dati venivano valutate solo manualmente. Nuovi

trat- tamenti possono essere sviluppati e adattati alle esigenze dei singoli pazienti, sulla base di confronti con masse di informazioni disponibili. Le imprese sper- ano che l'analisi dei megadati consentirà loro di ottenere vantaggi competitivi,

generare potenziali risparmi e creare nuovi settori commerciali attraverso un servizio clienti diretto e individualizzato. Le agenzie governative auspicano miglioramenti in materia di giustizia penale. La strategia per il mercato unico digitale in Europa della Commissione riconosce il potenziale delle tecnologie e dei servizi basati sui dati nonché dei Big Data quali catalizzatori di crescita eco- nomica, innovazione e digitalizzazione nell'UE[988].

Tuttavia, i megadati comportano anche dei rischi, generalmente associati ai loro attributi cosiddetti delle «tre V»: volume, velocità e varietà dei dati trat- tati. Il volume si riferisce alla quantità di dati trattati, la varietà al numero e alla diversità dei tipi di dati, mentre la velocità si riferisce alla rapidità del tratta- mento dei dati. Considerazioni specifiche per la protezione dei dati sorgono, in particolare, quando le analisi dei megadati vengono utilizzate su grandi insiemi di dati per estrarre conoscenze predittiva allo scopo di orientare processi deci- sionali con riferimento a persone e/o gruppi[989]. I rischi per la protezione dei dati e la vita privata correlati ai megadati sono stati posti in evidenza in pareri del GEPD e del Gruppo di lavoro articolo 29, in risoluzioni del Parlamento europeo e in documenti politici del Consiglio d'Europa[990].

I rischi possono includere il trattamento improprio dei megadati da parte di coloro che hanno accesso alla massa di informazioni, attraverso la manipolazi-

one, la discriminazione o l'oppressione di persone o gruppi specifici nella soci- età[991]. Quando vengono raccolte, trattate e valutate masse di dati o informazioni personali sul comportamento individuale, il loro sfruttamento può comportare violazioni significative dei diritti e delle libertà fondamentali, che vanno al di là

del diritto alla vita privata. Misurare esattamente in che misura la vita privata e i dati personali possono essere influenzati non è possibile. Il Parlamento europeo ha individuato la mancanza di una metodologia che consenta di effettuare una valutazione basata su riscontri oggettivi dell'impatto complessivo dei megadati, ma esistono elementi indicanti che l'analisi dei megadati può avere un impatto orizzontale significativo sia sul settore pubblico che su quello privato[992].

Il regolamento generale sulla protezione dei dati include disposizioni relative al diritto a non essere sottoposti a decisioni basate sul trattamento automatiz- zato, compresa la profilazione[993]. La questione della tutela della vita privata sorge quando l'esercizio del diritto all'opposizione richiede l'intervento umano, ottenere l'inter vento umano, permettendo agli interessati di esprimere la propria opinione e di contestare la decisione[994]. Ciò può comportare difficoltà nel garantire un livello adeguato di protezione dei dati personali qualora, ad esempio, non sia possibile un intervento umano o qualora gli algoritmi siano troppo complessi e la quantità di dati coinvolti troppo grande per giustificare determinate decisioni, e/o informazioni preliminari per ottenere il consenso degli interessati. Un esempio di utilizzo dell'IA e di processi decisionali autom- atizzati si ritrova nei recenti sviluppi nelle richieste di mutui o nell'ambito di processi di reclutamento. Le richieste

vengono rifiutate o scartate sulla base del fatto che i richiedenti non soddisfano parametri o fattori predeterminati.

10.1.3. Questioni relative alla protezione dei dati

In termini di protezione dei dati, le questioni principali riguardano, da un lato, il volume e la varietà dei dati personali trattati, dall'altro, il trattamento e i suoi risultati. L'introduzione di complessi algoritmi e software per trasformare i dati di massa in una risorsa al servizio di processi decisionali, incide in particolare sulle persone e i gruppi, segnatamente nei casi di profilazione o etichettatura e, in ultima analisi, solleva numerosi problemi in materia di protezione dei dati[995].

Identificazione dei titolari del trattamento e dei responsabili del trattamento e loro responsabilità

I megadati e l'IA sollevano diverse questioni con riferimento all'individuazione dei titolari del trat tamento e dei responsabili del trat tamento e alla loro responsabilità: quando viene raccolta e trattata una quantità così ingente di dati, chi ne è il proprietario? Quando i dati sono trattati da macchine di intel- ligenza artificiale o software, chi è il titolare del trattamento? Quali sono le responsabilità precise di ciascun attore nel trattamento dei dati? E per quali scopi possono essere usati i megadati?

La questione della responsabilità nell'ambito dell'IA diventerà ancora più complessa quando l'intelligenza artificiale prenderà decisioni basate sul trat- tamento di dati da essa stessa sviluppato. Il regolamento generale sulla pro- tezione dei dati fornisce un quadro giuridico per la responsabilità del titolare del trattamento e del responsabile del trattamento. Il trattamento illecito dei dati personali comporta la responsabilità del titolare del trattamento e del responsabile del trattamento[996]. L'intelligenza artificiale e il processo decision- ale automatizzato sollevano interrogativi su chi sia responsabile per le violazi- oni della vita privata degli interessati, quando la complessità e la quantità di dati trattati non possono essere attribuite con certezza. Se l'IA e gli algoritmi sono

considerati prodotti, sorgono problematiche tra la responsabilità person- ale, che è disciplinata dal regolamento generale sulla protezione dei dati, e la responsabilità per i danni da prodotti, che non lo è[997]. Ciò richiederebbe norme in materia di responsabilità, per colmare la lacuna tra responsabilità personale e responsabilità per il prodotto con riferimento alla robotica e all'intelligenza artificiale compreso, ad esempio, il processo decisionale automatizzato[998].

Impatto sui principi di protezione dei dati

La natura, l'analisi e l'utilizzo dei megadati come sopra descritti rendono ardua l'applicazione di alcuni principi fondamentali tradizionali del diritto europeo in

materia di protezione dei dati[999]. Tali sfide riguardano principalmente i prin- cipi di legittimità, di minimizzazione dei dati, di limitazione delle finalità e di trasparenza.

Il principio della minimizzazione dei dati prevede che i dati personali siano ade- guati, pertinenti e limitati a quanto necessario per le finalità del loro tratta- mento. Il modello operativo dei megadati, tuttavia, potrebbe essere l'antitesi della minimizzazione dei dati, dal momento che richiede una quantità sempre maggiore di dati, spesso per finalità non precisate.

Lo stesso vale per il principio della limitazione delle finalità, il quale richiede che i dati siano trattati per finalità specifiche e stabilisce che non possono essere utilizzati per scopi incompatibili con la finalità iniziale della raccolta, a meno che tale trattamento si basi su un fondamento giuridico come ad esem- pio, ma non solo, il consenso dell'interessato (cfr. sezione 4.1.1).

Infine, i megadati mettono in discussione anche il principio dell'esattezza dei dati, dal momento che le applicazioni di megadati tendono a raccogliere dati da una varietà di fonti, senza che sia possibile verificare e/o mantenere l'esattezza dei dati raccolti[1000].

Norme e diritti specifici

La regola generale rimane che i dati personali trattati attraverso l’analisi dei megadati rientrano nell’ambito di applicazione della legislazione in materia di protezione dei dati. Il diritto dell’UE, tuttavia, ha introdotto norme o deroghe specifiche per casi particolari in relazione al trattamento di dati algoritmici complessi. Nelle disposizioni del Consiglio d'Europa, la Convenzione modernz- zata n.108 garantisce nuovi diritti al soggetto titolare di dati in modo da per- mettere ad esso o ad essa di esercitare un controllo più efficace sui propri dati nell'era dei big data. Ad esempio, si tratta precisamente del caso riguardante l'Articolo 1(a), (c) e (d) della Convenzione Modernizzata, sul diritto del titolare di dati a non essere soggetto di decisioni rilevanti basate esclusivamente su

una gestione automatica dei propri dati, senza che il punto di vista del sog- getto sia stato preso in considerazione; il diritto di ottenere, previa richiesta, una chiarificazione sulle motivazioni che hanno portato all'utilizzo dei dati del soggetto così come il diritto di opporsi a tale utilizzo. Altre disposizioni della Convenzione modernizzata, in par ticolare in merito alla trasparenza e agli obblighi aggiuntivi sono elementi complementari del dispositivo di protezione stabilito con la Convenzione Modernizzata n.108 al fine di affrontare le nuove sfide digitali.

Nel diritto dell'UE, oltre ai casi elencati nell'articolo 23 del RGPD, la tras- parenza deve essere garantita per tutti i trattamenti di dati personali. Ciò è particolarmente importante con riferimento ai servizi Internet e ad altri comp- lessi processi automatizzati di trattamento dei dati, come l'uso di algoritmi nel processo decisionale. In questi casi, le caratteristiche dei sistemi di trat- tamento dei dati devono essere tali da consentire agli interessati di compren- dere realmente ciò che accade ai loro dati. Per garantire un trattamento cor- retto e trasparente, il regolamento generale sulla protezione dei dati richiede al titolare del trattamento di fornire all'interessato informazioni significative sulla logica utilizzata nei processi decisionali automatizzati, compresa la pro- filazione[1001]. Nella sua raccomandazione sulla protezione e la promozione del diritto alla libertà di

espressione e del diritto alla vita privata con riferimento alla neutralità della rete, il Comitato dei Ministri del Consiglio d'Europa ha rac- comandato che i fornitori di servizi Internet «forniscano agli utenti informazi- oni chiare, complete e pubbliche su tutte le prassi di gestione del traffico che potrebbero incidere sull'accesso degli utenti ai contenuti, applicazioni o servizi e sulla loro diffusione»[1002]. Relazioni sulle prassi di gestione del traffico Inter- net, redatte dalle autorità competenti di ciascuno Stato membro, dovrebbero essere redatte in modo aperto e trasparente e messe a disposizione del pub- blico gratuitamente[1003].

I titolari del trattamento devono informare gli interessati – che i dati siano o meno stati raccolti presso gli stessi – non solo in merito a informazioni

specifiche sui dati raccolti e sul trattamento previsto (cfr. sezione 6.1.1), ma anche, se del caso, in merito all'esistenza di processi decisionali automatizzati, fornendo loro «informazioni significative sulla logica utilizzata»[1004], sugli obiettivi e sulle potenziali conseguenze di tale trattamento. Il regolamento generale sulla protezione dei dati chiarisce anche che (solo nei casi in cui i dati personali non siano stati raccolti presso l'interessato) il titolare del trattamento non è tenuto a fornire tali informazioni all'interessato se «comunicare tali informazi- oni risulta impossibile o implicherebbe uno sforzo sproporzionato»[1005]. Tutta- via, come sottolineato dal Gruppo di lavoro articolo 29 nelle sue *linee guida in materia di processi decisionali automatizzati e profilazione ai fini del regola- mento n. 2016/679*, la complessità del trattamento non dovrebbe, di per sé, impedire al titolare del trattamento di fornire all'interessato spiegazioni chiare circa le finalità e le analisi utilizzate nel trattamento dei dati[1006].

I diritti degli interessati di accesso, rettifica e cancellazione dei loro dati per- sonali, nonché il loro diritto di limitare il trattamento, non prevedono una simile esenzione. Tuttavia, il titolare del trattamento può essere sollevato dall'obbligo di notificare l'interessato in caso di rettifica o cancellazione dei suoi dati personali (cfr. sezione 6.1.4) qualora tale notifica «si riveli impossibile o implichi uno sforzo sproporzionato»[1007].

Gli interessati hanno inoltre il diritto di opporsi, ai sensi dell'articolo 21 del RGPD (cfr. sezione 6.1.6), al trattamento dei dati personali che li riguardano, anche in caso di analisi dei megadati. I titolari del trattamento possono essere esentati da tale obbligo se sono in grado di dimostrare legit timi interessi d'ordine superiore, ma non possono beneficiare di tale esenzione in caso di trattamento dei dati a fini di marketing diretto.

Deroghe specifiche a tali diritti possono essere fatte valere anche dai titolari del trattamento quando i dati personali sono trattati per finalità di archiviazi- one nel pubblico interesse, per finalità di ricerca scientifica o storica o per final- ità statistiche[1008].

Per quanto riguarda la profilazione e i processi decisionali automatizzati, il RGPD ha introdotto norme specifiche: l'articolo 22, paragrafo 1, stabilisce che l'interessato «ha il diritto di non essere sottoposto a una decisione basata uni- camente sul trattamento automatizzato, [...] che produca effetti giuridici che lo riguardano». Come sottolineato dalle linee guida del Gruppo di lavoro arti- colo 29, tale articolo prevede un divieto generale dei processi decisionali inter- amente automatizzati[1009]. I titolari del trattamento possono essere esonerati da tale divieto solo in tre casi specifici: quando la decisione è 1) necessaria all'esecuzione di un contratto concluso tra l'interessato e il titolare del tratta- mento, 2) autorizzata dal diritto dell'UE o dal diritto nazionale o 3) basata sul consenso esplicito[1010].

Controllo individuale

La complessità dell'analisi dei megadati e la mancanza di trasparenza che la caratterizza possono richiedere un ripensamento del concetto di controllo indi- viduale dei dati personali. Questo dovrebbe essere adattato al contesto sociale e tecnologico attuale, tenendo conto della mancanza di conoscenza da parte degli individui. Pertanto, la protezione dei dati con riferimento ai megadati dovrebbe basarsi su un concetto più ampio di controllo sull'uso dei dati, in base al quale il controllo individuale dovrebbe evolvere in un processo più

comp- lesso, con molteplici valutazioni d’impatto dei rischi connessi all’uso dei dati[1011].

La qualità di un’applicazione di megadati dipende dalla capacità di prevedere i desideri o il comportamento delle persone (o dei consumatori) oggetto delle prove. Gli attuali modelli predittivi basati sull’analisi dei megadati vengono cos- tantemente perfezionati. I recenti sviluppi comprendono non solo l’utilizzo di dati per classificare le personalità (cioè il comportamento e gli atteggiamenti), ma anche lo studio del comportamento attraverso l’analisi di modelli vocali e dell’intensità con cui i messaggi vengono digitati, o della temperatura corporea. Ad esempio, tutte queste informazioni possono essere utilizzate in tempo reale in occasione di un incontro con un rappresentante di una banca per valutarne

l’affidabilità creditizia sulla base delle conoscenze tratte dalla valutazione dei megadati. La valutazione non si basa sul merito della persona che richiede il cred- ito, ma piuttosto sulle caratteristiche comportamentali che emergono dall’analisi e dalla valutazione dei megadati, ovvero il candidato che parla con una voce forte o lusinghiera, il suo linguaggio del corpo o la sua temperatura corporea.

La profilazione e la pubblicità mirata non costituiscono necessariamente un problema se le persone sono consapevoli di essere oggetto di pubblicità personalizzata. La profilazione diventa un problema quando viene utilizzata per manipolare le persone, ad esempio per cercare determinate personalità o gruppi di persone a fini di campagna politica. Ad esempio, gruppi di elet- tori indecisi possono essere contattati per mezzo di messaggi politici adattati alla loro «personalità» e ai loro atteggiamenti. Un’altra questione potrebbe essere l’utilizzo di tale profilazione per rifiutare l’accesso a prodotti e servizi a determinate persone. Una garanzia che può fornire protezione contro l’abuso dei megadati e delle informazioni personali è la pseudonimizzazione (cfr. sezione 2.1.1)[1012]. Se i dati personali sono realmente anonimizzati, vale a dire se non esistono informazioni che lasciano tracce legate all’interessato, tali casi non rientrano nell’ambito di applicazione del regolamento generale sulla protezione dei dati. Anche il consenso degli interessati e dei singoli al tratta- mento dei

megadati rappresenta una sfida per la legislazione in materia di pro- tezione dei dati. Questo include il consenso ad essere oggetto di pubblicità su misura e la profilazione, che possono essere giustificati con motivazioni legate all'«esperienza del cliente», e il consenso all'uso di masse di dati personali per perfezionare e sviluppare strumenti analitici basati su informazioni. La consa- pevolezza, o l'assenza di consapevolezza, del trattamento dei megadati solleva diversi interrogativi in relazione ai mezzi attraverso i quali gli interessati pos- sono esercitare i loro diritti, dato che il trattamento dei megadati può basarsi su informazioni oggetto di algoritmi sia pseudonimizzate, sia anonimizzate. Mentre i dati pseudonimizzati rientrano nell'ambito di applicazione del regola- mento generale sulla protezione dei dati, tale regolamento non si applica ai dati resi anonimi. Il controllo dell'individuo sul trattamento dei dati personali, e la sua consapevolezza in tal senso, sono fondamentali nell'analisi dei mega- dati: senza di essi, l'interessato non avrebbe un'idea chiara di chi sia il titolare del trattamento o il responsabile del trattamento, e non potrebbe esercitare efficacemente i propri diritti.

10.2. Web 2.0 e 3.0: i social network e l’Internet delle cose

- I servizi di social network (Social Networking Services - SNS) sono piattaforme di comunicazione on-line, che consentono alle persone di creare reti di utenti che condividono gli stessi punti di vista o di entrarne a far parte.

- L’Internet delle cose è la connessione di oggetti a Internet e l’interconnessione di oggetti tra di loro.

- Il consenso degli interessati è la base giuridica più comune per il trattamento lecito dei dati da parte dei titolari del trattamento sui social network.

- Gli utenti dei social network sono generalmente tutelati dall’«esenzione per l’esercizio di attività a carattere personale o domestico», tuttavia, tale deroga può essere revocata in contesti specifici.

- I fornitori di social network non sono tutelati dall’«esenzione per l’esercizio di attività a carattere personale o domestico».

- La protezione della vita privata fin dalla progettazione e la protezione per impostazione

predefinita sono essenziali per garantire la sicurezza dei dati in questo settore.

10.2.1. Definizione di Web 2.0 e 3.0

Servizi di social network

Inizialmente Internet era stato concepito come rete per interconnettere i com- puter e trasmettere messaggi con capacità limitate di scambio di dati, men- tre i siti web offrivano semplicemente la possibilità ai singoli di visualizzare passivamente i loro contenuti[1013]. Nell’era del Web 2.0, Internet si è trasfor- mato in un forum in cui gli utenti interagiscono, collaborano e generano input. Questa era è caratterizzata dallo straordinario successo e dall’utilizzo diffuso dei servizi di social network, che oggi sono un elemento essenziale della vita quotidiana di milioni di persone.

Il ser vizio di social network (SNS) o «social media» può essere definito in senso lato come una «piattaforma di comunicazione on-line che consente ad un utente di creare reti di utenti che condividono i suoi stessi interessi o di entrarne a far parte»[1014]. Per aderire a una rete o crearne una, gli individui sono invitati a fornire dati personali e a creare il proprio profilo. I servizi di social network permettono agli utenti di generare «contenuti» digitali, che vanno da fotografie e video, a link verso giornali e messaggi personali, per esprimere le proprie opinioni. Attraverso queste piattaforme online gli utenti possono interagire e comunicare con numerosi altri utenti. È importante sottolineare che la maggior parte dei servizi di social network non richiede alcun costo di iscrizione. Anziché chiedere agli utenti di pagare per entrare a far parte della rete, i fornitori di servizi di social network generano gran parte dei loro introiti attraverso la pubblicità mirata. Gli inserzionisti possono trarre enormi benefici dalle informazioni personali rivelate quotidianamente su questi siti. Avere a disposizione informazioni su età, sesso, ubicazione e interessi di un utente per- mette loro di raggiungere con i propri annunci le persone «giuste».

Esempio: Nora è molto felice perché il suo partner ha proposto il matrimonio. Vuole condividere la buona notizia con i suoi amici e familiari e decide di pubblicare un post emotivo su un social network,

esprimendo la sua gioia e di cambiare lo status della sua situazione sentimentale in «fidanzata». Nei giorni successivi, quando accede al suo account, Nora vede annunci su abiti da sposa e negozi di fiori. Perché succede questo?

Quando ha creato un annuncio su Facebook, le aziende che commercializzano in abiti da sposa e fiori hanno selezionato alcuni parametri per poter raggiungere persone come Nora. Se il suo profilo indica che è una donna, fidanzata, che vive a Parigi vicino alla zona dove si trovano i negozi di vestiti e fiori che pubblicano gli annunci, Nora vede immediatamente gli annunci.

L’Internet delle cose

L’Internet delle cose (Internet of Things - IoT) rappresenta il passo successivo nell’evoluzione di Internet: l’era del Web 3.0. Con l’Internet degli oggetti, i dis- positivi possono connettersi e interagire con altri dispositivi tramite Internet.

Ciò consente a oggetti e persone di essere interconnessi tramite reti di comuni- cazione, per segnalare il loro status e/o lo status dell’ambiente circostante[1015]. L’Internet degli oggetti e i dispositivi connessi sono già una realtà e se ne pre- vede una crescita sostanziale nei prossimi anni, con la creazione e l’ulteriore sviluppo di dispositivi intelligenti, che porteranno alla creazione di città intel- ligenti, abitazioni intelligenti e commerci intelligenti.

Il Comitato dei Ministeri del Consiglio d'Europa ha adottato una raccomandazi- one in merito alla tutela dei diritti umani nell'ambito dei servizi di social net- working[1016] che in una sezione specifica riguarda la protezione dei dati person- ali ed è stata integrata nel 2018 da un'ulteriore raccomandazione, incentrata sui ruoli e sulle responsabilità degli intermediari del web[1017].

Esempio: L’Internet delle cose può essere particolarmente vantaggioso per l’assistenza sanitaria. Alcune aziende hanno già creato dispositivi, sensori e applicazioni che consentono di monitorare la salute di un paziente. Attraverso l’utilizzo di un pulsante di allarme indossabile e altri sensori senza fili collocati intorno alla casa, è possibile seguire la routine quotidiana di persone anziane che vivono da sole e generare allarmi se vengono rilevate interruzioni significative nel loro programma giornaliero. I

sensori per il rilevamento delle cadute, ad esempio, sono ampiamente utilizzati dagli anziani. Questi sensori possono rilevare una caduta con precisione e informarne il medico e/o i famigliari della persona.

Esempio: Barcellona è uno degli esempi più noti di città intelligente. Dal 2012, la città ha adottato l'uso di tecnologie innovative con l'obiettivo di creare un sistema intelligente di trasporto pubblico, gestione dei rifiuti, parcheggio e illuminazione stradale. Per migliorare la gestione dei rifiuti, ad esempio, la città utilizza cassonetti intelligenti. Questi consentono il monitoraggio dei livelli dei rifiuti, per ottimizzare il percorso di raccolta. Quando i cassonetti sono quasi pieni, essi trasmettono segnali attraverso la rete di comunicazioni mobili, che vengono inviati all'applicazione software utilizzata dall'azienda

di gestione dei rifiuti. L'azienda può così pianificare il percorso migliore per la raccolta dei rifiuti, dando la priorità e/o semplicemente organizzando la raccolta dei bidoni che hanno effettivamente necessità di essere svuotati.

10.2.2. Bilanciamento dei vantaggi e dei rischi dei megadati

La vasta espansione e il successo dei servizi di social network negli ultimi dieci anni sono indicativi del fatto che producono benefici significativi. Ad esempio, la pubblicità mirata (come descritta nell'esempio evidenziato) è un modo par- ticolarmente innovativo per le aziende di raggiungere il loro pubblico, offrendo loro un mercato più specifico. Potrebbe rispondere anche all'interesse dei con- sumatori essere destinatari di annunci più pertinenti e interessanti. Ancora più importante, tuttavia, è il fatto che i servizi di social networking e i social media possono avere un impatto positivo sulla società e sull'attuazione di cambia- menti. Essi permettono agli utenti di comunicare, interagire, organizzare gruppi ed eventi su questioni che li riguardano.

Analogamente, si prevede che l'Internet degli oggetti apporterà notevoli ben- efici all'economia e rientra nella strategia dell'UE per lo sviluppo di un mercato unico digitale. All'interno dell'UE si stima che nel 2020 il numero di connessioni all'Internet degli

oggetti salirà a 6 miliardi. Si prevede che questa espansione della connettività por terà impor tanti benefici economici attraverso lo svi- luppo di servizi e applicazioni innovativi, una migliore assistenza sanitaria, una migliore comprensione delle esigenze dei consumatori e maggiore efficienza.

Al contempo, data l'enorme quantità di dati personali generati dagli utenti di social media e successivamente trattati dagli operatori di servizi, l'espansione dei servizi di social network suscita crescente preoccupazione circa le modal- ità con cui la vita privata e i dati personali possono essere protetti. I servizi di social network possono minacciare il diritto alla vita privata e il diritto alla libertà di espressione. Tali minacce possono includere: «l'assenza di garanzie giuridiche e procedurali in processi che possono condurre all'esclusione di un utente; la tutela inadeguata di minori e giovani nei confronti di contenuti o comportamenti suscettibili di recare loro pregiudizio; la mancanza di rispetto per i diritti altrui; l'assenza di una configurazione predefinita che rispetti la vita privata; la mancanza di trasparenza delle finalità per le quali i dati personali

sono raccolti e trattati»[1018]. La normativa europea in materia di protezione dei dati ha cercato di rispondere alle sfide poste dai social media con riferimento alla protezione della vita privata e dei dati personali. Principi quali il consenso, la protezione della vita privata e dei dati fin dalla progettazione e la protezione per impostazione predefinita rivestono particolare importanza nel contesto dei social media e dei servizi di networking.

Nell'ambito dell'Internet degli oggetti, le ingenti quantità di dati personali gen- erati dai diversi dispositivi interconnessi comportano rischi anche per la vita pri- vata e la protezione dei dati personali. Pur essendo la trasparenza un'importante principio del diritto europeo in materia di protezione dei dati, a causa della moltitudine di dispositivi connessi non sempre è chiaro chi sia in grado di rac- cogliere, accedere e utilizzare i dati raccolti dai dispositivi dell'Internet degli oggetti[1019]. Nondimeno, ai sensi del diritto dell'UE e del CdE, il principio di tras- parenza stabilisce l'obbligo per i titolari del trattamento di tenere informati gli interessati su come vengono utilizzati i loro dati, usando un linguaggio semplice e chiaro. Rischi, norme, garanzie e diritti relativi al trattamento dei loro dati personali devono essere indicati chiaramente agli interessati. I dispositivi con- nessi all'Internet degli oggetti e la molteplicità delle operazioni di trattamento e dei dati coinvolti potrebbero mettere in causa anche il requisito del consenso chiaro e

informato al trattamento dei dati, quando tale trattamento si basa sul consenso. Spesso le persone non comprendono il funzionamento tecnico di tale trattamento e quindi nemmeno le conseguenze del loro consenso.

Un’altra questione preoccupante è la sicurezza, dal momento che i dispositivi connessi sono particolarmente vulnerabili ai rischi relativi alla sicurezza. I dis- positivi connessi hanno diversi livelli di sicurezza. Poiché operano al di fuori dell’infrastruttura IT standard, potrebbero non disporre della capacità di elabo- razione e memorizzazione adeguata per ospitare software di sicurezza o utiliz- zare tecniche quali la crittografia, la pseudonimizzazione o l’anonimizzazione per proteggere i dati personali degli utenti.

Esempio: in Germania, le autorità di regolamentazione hanno deciso di vietare un giocattolo connesso a Internet a seguito di serie preoccupazioni

circa l'impatto del giocattolo sul rispetto della vita privata dei bambini. Le autorità di regolamentazione hanno ritenuto che una bambola connessa a Internet, di nome Cayla, costituiva di fatto un dispositivo di spionaggio nascosto. La bambola funzionava trasmettendo le domande audio del bambino a un'applicazione su un dispositivo digitale, che le traduceva in testo e cercava una risposta in Internet. L'applicazione inviava quindi una risposta alla bambola, che la comunicava vocalmente al bambino. Attraverso questa bambola, le comunicazioni del bambino, nonché quelle degli adulti nelle vicinanze, potevano essere registrate e trasmesse all'applicazione. Se i produttori della bambola non avessero adottato misure di sicurezza adeguate, la bambola avrebbe potuto essere utilizzata da chiunque per ascoltare le conversazioni.

10.2.3. Questioni relative alla protezione dei dati

Consenso

In Europa, il trattamento dei dati personali è lecito solo se è consentito dalla normativa europea in materia di protezione dei dati. Per i fornitori di servizi di social network, il consenso degli interessati costituisce, di norma, una base giuridica per il trattamento dei dati. Il consenso deve essere prestato libera- mente ed essere specifico,

informato ed inequivocabile (cfr. sezione 4.1.1)[1020].

«Liberamente prestato» significa sostanzialmente che gli interessati devono essere in grado di operare una scelta reale e autentica. Il consenso è «specif- ico» e «informato» quando è comprensibile, fa riferimento con chiarezza e pre- cisione alla portata effettiva, alle finalità e alle conseguenze del trattamento dei dati. Nell'ambito dei social media, è lecito chiedersi se il consenso sia libero, specifico e informato per tutti i tipi di trattamento effettuati dall'operatore dei servizi di social network ed a terzi.

Esempio: Spesso, per aderire e accedere a un servizio di social network, gli individui devono rilasciare un'autorizzazione a forme diverse di trattamento dei loro dati personali, non di rado senza la possibilità di ricevere i necessari chiarimenti o avere opzioni alternative. Un esempio potrebbe essere costituito dalla necessità di prestare il proprio consenso a ricevere pubblicità comportamentale per potersi registrare a un servizio di social network. Come

rilevato dal Gruppo di lavoro articolo 29 nel suo parere sulla definizione di consenso, «[c]onsiderando l'importanza acquisita da alcuni social network, talune categorie di utenti (come gli adolescenti) accetteranno di ricevere messaggi di pubblicità comportamentale per evitare il rischio di essere parzialmente esclusi dalle interazioni sociali. L'utente dovrebbe essere messo in condizione di dare un consenso libero e specifico in merito all'invio di messaggi di pubblicità comportamentale, indipendentemente dall'accesso al servizio di social network»[1021].

Ai sensi del regolamento generale sulla protezione dei dati, i dati personali dei minori di 16 anni non possono, in linea di principio, essere trattati sulla base del loro consenso[1022]. Se per il trattamento è necessario il consenso, questo deve essere dato dal genitore o dal tutore del minore. I minori meritano una specifica protezione in quanto possono essere meno consapevoli dei rischi e delle conseguenze in relazione al trattamento dei dati personali. Ciò è molto importante nel contesto dei social media, dal momento che i minori sono più vulnerabili ad alcuni degli effetti negativi che l'utilizzo di tali media può com- portare, come il cyberbullismo, gli atti persecutori on-line (cyber-stalking), o il furto d'identità.

Sicurezza e protezione della vita privata/dei dati fin dalla progettazione e per impostazione predefinita

Il trattamento dei dati personali comporta intrinsecamente rischi per la sicurezza, data la costante possibilità che una violazione della sicurezza com- porti la distruzione accidentale o illegale, la perdita, la modifica, l'accesso o la rivelazione non autorizzati ai dati personali trattati. Nell'ambito del diritto europeo in materia di protezione dei dati, i titolari del trattamento e i respon- sabili del trattamento sono tenuti ad attuare misure tecniche e organizzative adeguate per prevenire ogni ingerenza non autorizzata nelle operazioni di trat- tamento dei dati. Anche i fornitori di servizi di social network che rientrano nell'ambito di applicazione della normativa europea in materia di protezione dei dati devono conformarsi a questo obbligo.

I principi di protezione della vita privata e dei dati fin dalla progettazione e per impostazione predefinita, impongono ai titolari del trattamento di garantire la sicurezza fin dalla progettazione dei loro prodotti e di applicare automatica- mente impostazioni adeguate in materia di protezione della vita privata e dei dati. Ciò significa che quando una persona decide di aderire a un social net- work, il fornitore di servizi può non mettere automaticamente a disposizione di tutti i suoi utenti tutte le informazioni riguardanti il nuovo utente del servizio. Quando si accede al servizio, le impostazioni predefinite relative alla vita pri- vata e alla protezione dei dati dovrebbero essere tali da rendere le informazi- oni disponibili solo ai contatti selezionati dall'utente. L'estensione dell'accesso a persone al di fuori di tale elenco dovrebbe essere possibile solo dopo che l'utente abbia provveduto a modificare manualmente le impostazioni predefi- nite di protezione dei dati e della vita privata. Ciò può avere un impatto anche nei casi in cui si verifichi una violazione dei dati personali malgrado le misure di sicurezza adottate. In questi casi, i fornitori del servizio devono notificare gli utenti interessati qualora la violazione dei dati personali sia suscettibile di pre- sentare un rischio elevato per i diritti e le libertà dell'interessato[1023].

La protezione della vita privata e dei dati fin dalla progettazione e la protezi- one per impostazione predefinita rivestono particolare importanza

nell’ambito dei servizi di social network poiché, oltre al rischio di accesso non autorizzato insito nella maggior parte dei tipi di trattamento, la condivisione di informazi- oni personali nei social media pone rischi supplementari per la sicurezza. Essi sono spesso dovuti alla mancanza di comprensione da parte degli individui riguardo a *chi* può accedere alle loro informazioni e a come tali persone potreb- bero usarle. Con la diffusione dell’uso dei social media, il numero di casi di furto d’identità e di vittime è aumentato.

Esempio: il furto di identità è un fenomeno per cui una persona ottiene informazioni, dati o documenti appartenenti ad un’altra persona (la vittima) e utilizza poi tali informazioni per impersonare la vittima ed ottenere prodotti e servizi in suo nome. Si prenda ad esempio Paul, che ha un account su un sito di social media. Paul è un insegnante e membro attivo della sua comunità, molto estroverso e non particolarmente preoccupato delle impostazioni del suo account di social media riguardanti la riservatezza e la protezione dei dati. Ha un nutrito elenco di contatti, che include talvolta anche persone che non conosce necessariamente di persona. Poiché lavora in un vasto

complesso scolastico ed è piuttosto popolare come allenatore della squadra di calcio della scuola, pensa che queste persone siano probabilmente genitori o amici della scuola. L'indirizzo email e la data di nascita di Paul sono visibili nel suo account di social media. Inoltre, Paul pubblica regolarmente foto del suo cane Toby, accompagnate da commenti come «Toby ed io durante la nostra corsa mattutina». Paul non si è reso conto che una delle domande di sicurezza più frequenti per proteggere il proprio account di posta elettronica o di telefonia cellulare è «Qual è il nome del vostro animale domestico». Utilizzando le informazioni disponibili nel profilo di social media di Paul, Nick riesce facilmente a piratare gli account di quest'ultimo.

Diritti delle persone

I fornitori di ser vizi di social net work devono rispet tare i dirit ti delle per- sone (cfr. la sezione 6.1), compreso il diritto di essere informati sulla final- ità del trattamento e su come i dati personali possono essere utilizzati per scopi di marketing diretto. Alle persone deve altresì essere accordato il diritto di accedere ai dati personali che hanno generato nella piattaforma di social network e di chiedere la loro cancellazione. Anche quando le persone abbi- ano acconsentito al trattamento dei loro dati personali e abbiano caricato informazioni on-line, devono beneficiare del «diritto all'oblio»

qualora non intendano più ricevere i ser vizi del social network. Il diritto alla portabilità dei dati consente inoltre agli utenti di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, una copia dei dati personali trasmessi al fornitore dei servizi di social network e di trasferirli da un forni- tore di social network ad un altro[1024].

Titolari del trattamento

Una domanda difficile che ricorre spesso nel contesto dei social media è la questione di chi sia il titolare del trattamento, vale a dire, la persona sulla quale incombono l'obbligo e la responsabilità di osservanza delle norme in materia di protezione dei dati. I fornitori di servizi di social network sono considerati tito- lari del trattamento nell'ambito del diritto europeo sulla protezione dei dati. Ciò è evidente data l'ampia definizione di «titolare del trattamento» e il fatto che tali fornitori di servizi determinano la finalità e i mezzi per il trattamento dei

dati personali condivisi dalle persone. Nell'ambito del diritto dell'UE, qualora offrano servizi agli interessati nell'UE, i titolari del trattamento sono tenuti ad osservare le disposizioni del regolamento generale sulla protezione dei dati anche se non sono stabiliti nell'UE.

Ma anche gli utenti dei servizi di social network possono essere considerati titolari del trattamento? In caso di trattamento di dati personali «nell'ambito di attività a carattere esclusivamente personale o domestico», le norme sulla pro- tezione dei dati non si applicano. Nell'ambito del diritto europeo in materia di protezione dei dati, tale nozione è conosciuta come «esenzione per l'esercizio di attività a carattere personale o domestico». Tuttavia, in alcuni casi, un utente di un servizio di social network può non rientrare in tale categoria.

Gli utenti condividono volontariamente i loro dati personali on-line. Tuttavia, le informazioni condivise on-line spesso includono informazioni personali riguar- danti altre persone.

Esempio: Paul ha un account su una piattaforma di social networking molto conosciuta. Vorrebbe diventare attore e utilizza il suo account per pubblicare foto, video e messaggi che illustrano la sua passione per l'arte. La popolarità è importante per il suo futuro; ha quindi deciso di mettere il suo profilo

a disposizione non solo dell'elenco dei suoi contatti più stretti, ma di tutti gli utenti di Internet, che siano o meno membri della rete. Paul può pubblicare foto e video di se stesso insieme alla sua amica Sarah senza il consenso di quest'ultima? In qualità di maestra elementare, Sarah cerca di tenere la sua vita privata lontano dal suo datore di lavoro, dai suoi allievi e dai loro genitori. Si immagini un esempio in cui Sarah, che non utilizza i social network, scopre dal loro comune amico Nick che una foto di lei ad una festa con Paul è stata pubblicata on-line. In questo caso, il trattamento dei dati di Paul non rientra nell'ambito di applicazione del diritto dell'UE dal momento che è soggetto all'«esenzione per l'esercizio di attività a carattere personale o domestico».

Tuttavia, è fondamentale che gli utenti siano coscienti e consapevoli del fatto che pubblicare online informazioni riguardanti altre persone senza il loro con- senso può violare il diritto alla vita privata e alla protezione dei dati di tali per- sone. Anche qualora l'esenzione per l'esercizio di attività a carattere personale o domestico sia applicabile (ad esempio se un utente ha un profilo reso pub- blico solo ad un elenco di contatti selezionati dallo stesso), la pubblicazione

di informazioni personali riguardanti terzi può comunque implicare la respon- sabilità dell'utente. Sebbene le norme in materia di protezione dei dati non si applichino in caso di esenzione per l'esercizio di attività a carattere person- ale o domestico, la responsabilità potrebbe sorgere dall'applicazione di altre norme nazionali, come nel caso della diffamazione o della violazione dei diritti della personalità. Infine, solo gli utenti dei servizi di social network sono tute- lati dall'esenzione per l'esercizio di attività a carattere personale o domestico: i titolari del trattamento e i responsabili del trattamento che forniscono i mezzi per tale trattamento privato dei dati, rientrano nell'ambito di applicazione del diritto europeo in materia di protezione dei dati[1025].

In seguito alla riforma della Direttiva alla vita privata e alle comunicazi- oni elettroniche, le norme sulla protezione dei dati, sulla vita privata e sulla sicurezza applicabili ai fornitori di servizi di telecomunicazione nell'ambito dell'attuale quadro giuridico si applicheranno anche ai servizi di comunicazione da macchina a macchina e di comunicazione elettronica, inclusi ad esempio i servizi over-the-top.